Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory

Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory

A dissertation presented

by

Nathan Kaplan

to

The Department of Mathematics

in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics

Harvard University
Cambridge, Massachusetts

April 2013

Dissertation Advisor: Professor Noam Elkies Nathan Kaplan

Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory

Abstract

The goal of this thesis is to apply an approach due to Elkies to study the distribution of rational point counts for certain families of curves and surfaces over finite fields. A vector space of polynomials over a fixed finite field $\mathbb{F}_q$ gives rise to a linear code, and the weight enumerator of this code gives information about point count distributions. The MacWilliams theorem gives a relation between the weight enumerator of a linear code and the weight enumerator of its dual code.

For certain codes C coming from families of varieties where it is not known how to determine the distribution of point counts directly, we analyze low-weight codewords of the dual code and apply the MacWilliams theorem and its generalizations to gain information about the weight enumerator of C. These low-weight dual codes can be described in terms of point sets that fail to impose independent conditions on this family of varieties.

Our main results concern rational point count distributions for del Pezzo surfaces of degree 2, and for certain families of genus 1 curves. These weight enumerators have interesting geometric and coding theoretic applications for small q.

Contents

Acknowledgements

I thank my advisor, Noam Elkies, for his guidance and support throughout this project and his incredibly generosity with his time and his ideas. I also thank Henry Cohn and Joe Harris for helpful discussions and for being valuable mentors throughout my time in graduate school. Ramin Takloo-Bighash, Scott Chapman, and Joe Gallian have also played important roles in my development during graduate school and have given me great advice and encouragement.

I thank Nathan Pflueger and Ian Petrow for helpful discussions and comments related to this project. I thank Alexander Barg, Thomas Britz, Irfan Siap, and two anonymous referees for comments that helped improve Chapter 5. I thank Abhinav Kumar for being a member of my thesis committee.

I thank Susan Gilbert and the rest of the staff of the Harvard math department for all of the valuable work that they do to make the graduate program run smoothly. I thank Robin Gottlieb and the preceptor staff for the thought and energy they put into the teaching program. They have created a very positive environment to help me and the other graduate students develop as educators.

I thank the NSF for supporting me with a Graduate Research Fellowship.

Finally, I thank my parents and Amie Sugarman for their support and encouragement.

CHAPTER 1

Introduction

The main goal of this thesis is to apply an approach of Elkies using coding theory to understand the distribution of rational point counts for a family of varieties over a finite field [**20**]. In particular, we focus del Pezzo surfaces and certain families of genus 1 curves. A vector space of polynomials gives a linear code, a linear subspace of $\mathbb{F}_q^N$ for some N, and studying properties of this code will answer questions about the distribution of rational point counts. The major coding theoretic tool that we use is the relationship between a linear code C and its dual code $C^\perp$, specifically the relationship between their weight enumerators given by the MacWilliams theorem. We prove several variations of the MacWilliams theorem that let us gain new information about point counts.

We first state the problem in the language of algebraic geometry. Let V be a variety over a finite field $\mathbb{F}_q$ and let $L \to V$ be a line bundle. We choose an M-dimensional space C of sections of L. We also require that there is no nonzero $c \in C$ that vanishes on all of $V(\mathbb{F}_q)$. Then C gives a map $\varphi : V(\mathbb{F}_q) \to \mathbb{P}^{M-1}(\mathbb{F}_q)$. As we vary over all $c \in C$, what is the distribution of the number of points of $\{p \in V(\mathbb{F}_q) \mid c(p) = 0\}$? We study C as a linear subspace of $\mathbb{F}_q^N$ where $N = \#V(\mathbb{F}_q)$. A linear subspace of $\mathbb{F}_q^N$ is also known as a linear code. For example we consider $V = \mathbb{P}^n(\mathbb{F}_q)$, $L = \mathcal{O}(d)$, and $C = \Gamma(L)$ (homogeneous degree d polynomials on $\mathbb{P}^n$) and get a linear code over $\mathbb{F}_q^N$ where $N = (q^{n+1} - 1)/(q - 1)$. In other parts of this thesis V will not be a projective space but some other variety, for example $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ or a smooth quadric in $\mathbb{P}^4(\mathbb{F}_q)$.

We now give some of the key definitions in coding theory that will play a major role throughout this thesis.

Definition. *A* code C *is a subset of* $\mathbb{F}_q^N$. *We say that* C *is a* linear code *if* C *is a linear subspace, that is, for all* $c_1, c_2 \in C$ *we have* $c_1 + c_2 \in C$ *and* $ac \in C$ *for all* $a \in \mathbb{F}_q$.

For $x, y \in \mathbb{F}_q^N$ *define the* Hamming distance $d(x, y)$ *as the number of coordinates in which they differ. That is, if* $x = (x_1, x_2, \ldots, x_N)$ *and* $y = (y_1, y_2, \ldots, y_N)$ *then*

$$d(x, y) = \#\{i \ \text{ such that } x_i \neq y_i, \ 1 \leq i \leq N\}.$$

For $x \in \mathbb{F}_q^N$ *we define* $\mathrm{wt}(x)$, *the* weight *of* x, *to be* $d(x, 0)$, *the number of nonzero coordinates of* x.

In this thesis we study codes coming from the evaluation of polynomials. Given a polynomial f, the weight of the codeword associated to f gives the number of zeros of the variety cut out by f. Our goal is to understand how these counts vary as we consider all of the polynomials in a given vector space. Therefore, it will be convenient to have a way to keep track of the distribution of weights that occur in a code C.

Definition. *The* Hamming weight enumerator *of a code* C *is a homogeneous polynomial*

$$W_C(X, Y) = \sum_{c \in C} X^{N - \mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{N} A_i X^{N-i} Y^i,$$

where

$$A_i = \#\{c \in C \ \text{ such that } \mathrm{wt}(c) = i\}.$$

This project builds heavily on work of Elkies [**20**] in which he determines the Hamming weight enumerator for the code of homogeneous cubics in $\mathbb{P}^3(\mathbb{F}_q)$. In the language of the paragraph above, this is the code with $V = \mathbb{P}^3(\mathbb{F}_q)$, $L = \mathcal{O}(3)$, and

C its space of global sections. More concretely, consider the q^{20} homogeneous cubic polynomials $f_3(w, x, y, z)$ on $\mathbb{P}^3(\mathbb{F}_q)$, which has $N := q^3 + q^2 + q + 1$ points. It does not really make sense to evaluate a polynomial at point of $\mathbb{P}^3$ since the coordinates of such a point are defined only up to scalar multiplication, but whether a polynomial evaluated at a point is zero or nonzero does not depend on the scalar multiple chosen. By fixing an affine representative for each projective point and choosing some ordering for these N points, evaluation now gives a well defined map taking a polynomial to an element of $\mathbb{F}_q^N$. Changing the choice of affine representatives gives an equivalent code.

The goal is to determine for each $t \in [0, N]$, how many of these cubics have t zeros. This is exactly the information contained in the Hamming weight enumerator of C. The zeros of a cubic polynomial f_3 are the $\mathbb{F}_q$-points of the variety given by $f_3(w, x, y, z) = 0$, so this problem is equivalent to understanding the distribution of the number of $\mathbb{F}_q$-points for this family of varieties.

There is a dual code $C^\perp$ associated to a linear code $C \subset \mathbb{F}_q^N$, and studying properties of this dual code often helps lead to a better understanding of C. We being with some definitions.

Definition. *Let $x = (x_1, \ldots, x_N)$ and $y = (y_1, \ldots, y_N)$ be two elements of $\mathbb{F}_q^N$. Define a pairing*

$$\langle \cdot, \cdot \rangle : \ \mathbb{F}_q^N \times \mathbb{F}_q^N \to \mathbb{F}_q^N$$

by

$$\langle x, y \rangle := \sum_{i=1}^{N} x_i y_i.$$

Given a linear code C we define the dual code

$$C^\perp := \{y \in \mathbb{F}_q^N : \ \forall x \in C, \ \langle x, y \rangle = 0\}.$$

Throughout this thesis we study a linear code C by studying properties of the dual code $C^\perp$. The MacWilliams theorem of coding theory allows us to draw conclusions about the weight enumerator of C given information about the weights of codewords of $C^\perp$. In fact, the weight enumerator of C completely determines the weight enumerator of $C^\perp$ and vice versa [**33**]. In Chapter 3 we give a proof of the following theorem using discrete Poisson summation.

Theorem 1 (MacWilliams)**.** *Let C be a linear code over $\mathbb{F}_q^N$. Then*

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y).$$

In order to determine the weight enumerator of a linear code C, it suffices to compute the weight enumerator of $C^\perp$. Since the codewords of C come from evaluating polynomials, the codewords of the dual code $C^\perp$ are also related to the geometry of projective space. We define the *support* of a codeword c to be the set of points p in $\mathbb{P}^n(\mathbb{F}_q)$ such that the coordinate of c corresponding to p is nonzero. If C is a code that comes from the evaluation of polynomials, then codewords of $C^\perp$ have supports that fail to impose independent conditions on these polynomials, that is, the dimension of the space of polynomials vanishing at these points exceeds what we expect for generically chosen points. With the description given above, points imposing dependent conditions are subsets $S \subset \mathbb{P}^n(\mathbb{F}_q)$ for which $\varphi(S)$ is linearly dependent.

This is the subject of interpolation problems in algebraic geometry: given a variety V and a vector space of polynomials, describe all configurations of n points of V that fail to impose independent conditions on these polynomials. It is often easier to count point sets failing to impose independent conditions than it is to count rational points on varieties directly. This gives information about the possible supports of dual codewords, and the MacWilliams theorem lets us draw conclusions about distributions of rational point counts.

We give an example from [**20**] to motivate this kind of analysis. We denote the code of homogeneous degree d forms on $\mathbb{P}^n(\mathbb{F}_q)$ by $C_{n,d}$. Consider the code $C_{n,1}$ of linear forms on $\mathbb{P}^n(\mathbb{F}_q)$. Linear forms give an $n+1$ dimensional vector space, and evaluation gives a map to $\mathbb{F}_q^N$ where $N = (q^{n+1}-1)/(q-1)$. Every nonzero linear form defines a hyperplane in $\mathbb{P}^n(\mathbb{F}_q)$ that has $(q^n-1)/(q-1)$ $\mathbb{F}_q$-rational points. Therefore the weight enumerator of this code is given by

$$W_{C_{n,1}}(X,Y) = X^N + (q^{n+1}-1)X^{N-q^n}Y^{q^n}.$$

Applying the MacWilliams theorem shows that

$$W_{C_{n,1}^\perp}(X,Y) = X^N + \frac{(q^{n+1}-1)(q^n-1)q}{6}X^{N-3}Y^3 + O(Y^4).$$

We see that the number of weight 3 codewords of the dual code is exactly $q-1$ times the number of triples of collinear points in $\mathbb{P}^n(\mathbb{F}_q)$. It is not difficult to check that every collinear triple occurs as the support of exactly $q-1$ codewords, and that these are the only possible supports.

We explain in more detail how the supports of dual codewords relate to points that fail to impose independent conditions in the case of linear forms on $\mathbb{P}^2(\mathbb{F}_q)$. Suppose we have $c \in C_{2,1}^\perp$ of weight three. There are three nonzero coordinates of c, a_i, a_j, a_k, and each coordinate corresponds to a point in $\mathbb{P}^2(\mathbb{F}_q)$. We have

$$a_i f(p_i) + a_j f(p_j) + a_k f(p_k) = 0,$$

for all linear forms $f(x,y,z)$. Since $a_i f(p_i) + a_j f(p_j) = -a_k f(p_k)$, the value of $f(p_k)$ can be determined from the value of $f(p_i)$ and $f(p_j)$. In particular, it is not possible for $f(x,y,z)$ to vanish on the points p_i and p_j, but be nonzero at p_k. Therefore, these points are collinear. They fail to impose independent conditions on linear forms because we do not expect any linear form to vanish on three generic points, but for collinear points such a form does exist.

A dual codeword carries more information than just the fact that the support corresponds to points failing to impose independent conditions. It explicitly gives a linear relation among values of these functions taken at these points. Suppose $p_1, \ldots, p_4$ are four points of a line $L \subset \mathbb{P}^2(\mathbb{F}_q)$ and p_5 is a point not on L. Bézout's theorem implies that a conic intersecting a line at 4 points must contain that line. Generically, given five points there is a unique conic containing them, but here we have all conics consisting of L together with a line through p_5. So, these points fail to impose independent conditions on degree 2 polynomials in $\mathbb{P}^2(\mathbb{F}_q)$.

Suppose we have a dual codeword c with support $p_1, \ldots, p_5$. For concreteness we suppose that L is given by the line $z = 0$ and $p_5 = (0, 0, 1)$, the affine representative of $[0 : 0 : 1]$. The nonzero coordinates of c are coefficients a_i satisfying

$$\begin{aligned} \sum_{i=1}^{5} a_i f(p_i) &= a_5 f(p_5) + \sum_{i=1}^{4} a_i f(p_i) = 0, \quad \text{for all} \\ f(x, y, z) &= b_1 x^2 + b_2 xy + b_3 xz + b_4 y^2 + b_5 yz + b_6 z^2. \end{aligned}$$

This implies

$$a_5 b_6 + \sum_{i=1}^{4} a_i f(p_i) = 0.$$

The terms $f(p_i)$ for each i satisfying $1 \leq i \leq 4$ are linear combinations of the coefficients b_1, b_2, and b_4. The only way for this equality to hold for all $f(x, y, z)$ is for $a_5 = 0$. These points fail to impose independent conditions, so we can find dual codewords supported on them. We have seen that every linear relation supported on these points has $a_5 = 0$. Throughout this thesis we will be interested in counting dual codewords of given weight, and will need to do more than just determine the point sets failing to impose independent conditions.

The family of codes arising from evaluation of polynomials contains some famous examples from coding theory. This code of linear forms on $\mathbb{P}^n(\mathbb{F}_q)$ is the q-ary Simplex Code of dimension $n + 1$, an interesting object that arises in other areas of coding

theory and has other constructions [**26**]. Its dual is the more famous q-ary Hamming code, one of the most studied objects in coding theory. This construction of these famous codes in terms of linear forms on $\mathbb{P}^n(\mathbb{F}_q)$ lets us study them using the geometry of $\mathbb{P}^n(\mathbb{F}_q)$.

A common theme of this thesis will be the use of refinements of the classical Hamming weight enumerator that keep track of more information about a code to draw conclusions about rational points. We give such an example in the setting of linear forms on $\mathbb{P}^2(\mathbb{F}_q)$.

Definition. *We define the* 2-tuple weight enumerator *of a code* $C \subseteq \mathbb{F}_q^N$ *by*

$$W_C^{[2]}(X,Y) = \sum_{i=0}^{N} B_i X^{N-i} Y^i,$$

where B_i *is equal to the number of pairs of codewords* $x, y \in C$ *with* $x = (x_1, \ldots, x_N)$ *and* $y = (y_1, \ldots, y_N)$ *such that there are* $N - i$ *coordinates for which* $x_j = y_j = 0$.

This weight enumerator tells us about the common zeros among pairs of codewords drawn from the same code. If a code C comes from the evaluation of some vector space of polynomials, then its 2-tuple weight enumerator gives information about the distribution of counts for common zeros of pairs of polynomials in this space. This tells us about the counts for rational points on complete intersections of codimension 2.

As a first example, consider the code $C_{2,1}$ of linear forms on $\mathbb{P}^2(\mathbb{F}_q)$. We have already seen that

$$W_{C_{2,1}}(X,Y) = X^{q^2+q+1} + (q^3-1)X^{q+1}Y^{q^2}.$$

A simple calculation gives the 2-tuple weight enumerator

$$W_{C_{2,1}}^{[2]}(X,Y) = X^{q^2+q+1} + (q^2-1)(q^2+q+1)X^{q+1}Y^{q^2} + (q-1)^2(q^2+q+1)XY^{q^2+q},$$

since any pair of distinct $\mathbb{F}_q$-rational lines intersect in a unique point of $\mathbb{P}^2(\mathbb{F}_q)$.

The MacWilliams theorem extends to this 2-tuple weight enumerator and to other generalizations. In Chapter 5 we will develop the theory of these higher weight enumerators, and in Chapter 6 we will use them to study certain codes coming from varieties.

Proposition 2. *Let C be a linear code over $\mathbb{F}_q^N$. Then*

$$W_{C^\perp}^{[2]}(X,Y) = \frac{1}{|C|^2} W_C^{[2]}(X + (q^2-1)Y, X - Y).$$

In this particular case, we see that

$$\begin{aligned} W_{C_{2,1}^\perp}^{[2]}(X,Y) &- (q+1)(W_{C_{2,1}^\perp}(X,Y) - X^{q^2+q+1}) - X^{q^2+q+1} \\ &= \frac{(q-2)(q-1)^3 q^2 (q+1)^2 (q^2+q+1)}{24} X^{q^2+q-2} Y^3 + O(Y^4). \end{aligned}$$

This is $(q-1)^2 q(q+1)$ times the number of collections of four collinear points in $\mathbb{P}^2(\mathbb{F}_q)$, the number of choices of a basis for a 2-dimensional subspace of $C_{2,1}^\perp$ that is spanned by two codewords of weight three such that the union of their supports is four collinear points. We will explain this type of result in further detail in Chapter 6.

The Hamming weight enumerator keeps track only of the number of coordinates of a codeword that are zero and the number that are nonzero. All nonzero coordinates are treated the same. Much of this thesis is focused on counting points on varieties expressed as double covers of $\mathbb{P}^1$ and of $\mathbb{P}^2$, so it will be useful to distinguish between coordinates that are nonzero squares in $\mathbb{F}_q^*$ and coordinates that are non-squares of $\mathbb{F}_q^*$.

Definition. *For a field $\mathbb{F}_q$ of characteristic not equal to 2, let $r(q)$ denote the set of squares in $\mathbb{F}_q^*$ and $s(q)$ denote the set of non-squares in $\mathbb{F}_q^*$. For $x = (x_1, \ldots, x_N) \in \mathbb{F}_q$*

we define

$$\mathrm{Res}(x) = \#\{i \quad \textit{such that } x_i \in r(q)\}, \quad \textit{and } \mathrm{NRes}(x) = \#\{i \quad \textit{such that } x_i \in s(q)\}.$$

We see that $\mathrm{Res}(x) + \mathrm{NRes}(x) = \mathrm{wt}(x)$.

Given a linear code $C \subset \mathbb{F}_q^N$ *we define the* quadratic residue weight enumerator *of* C *to be the homogeneous polynomial in three variables defined by*

$$\mathrm{QR}_C(X, Y, Z) = \sum_{c \in C} X^{N-\mathrm{wt}(c)} Y^{\mathrm{Res}(c)} Z^{\mathrm{NRes}(c)}.$$

We first give an example of an application of this weight enumerator. Consider homogeneous quadratic polynomials on $\mathbb{P}^1(\mathbb{F}_q)$, binary quadratic forms, $C_{1,2}$. It is a simple exercise to write down the weight enumerator of this three-dimensional code:

$$W_{C_{1,2}}(X, Y) = X^{q+1} + \frac{(q+1)q(q-1)}{2} X^2 Y^{q-1} + (q-1)(q+1) X Y^q + \frac{(q-1)^2 q}{2} Y^{q+1}.$$

Suppose we are interested in knowing the distribution of point counts for $w^2 = f_2(x, y)$ as $f_2(x, y)$ varies over all homogeneous quadratic polynomials. This is equivalent to knowing $\mathrm{QR}_{C_{1,2}}(X, X^2, 1)$. In this case the quadratic residue weight enumerator is not difficult to determine, as each such variety defines a conic in $\mathbb{P}^2(\mathbb{F}_q)$. There are two types of points on this variety, those that come from $w = 0$ and $f_2(x, y) = 0$, and pairs of points coming from points for which $f_2(x, y)$ is a nonzero square. We can gain extra information by keeping track of these counts separately.

We note that any quadratic polynomial $f_2(x, y)$ on $\mathbb{P}^1(\mathbb{F}_q)$ with two distinct roots defines a variety $w^2 = f_2(x, y)$ in $\mathbb{P}^2(\mathbb{F}_q)$ that is a smooth conic. This does not depend on whether the two roots are $\mathbb{F}_q$-rational or a pair of Galois-conjugate points defined over $\mathbb{F}_{q^2}$. All smooth conics are equivalent under automorphisms of $\mathbb{P}^2(\mathbb{F}_q)$ and in particular, have $q + 1$ $\mathbb{F}_q$-rational points. If $f_2(x, y)$ has a double zero, then $w^2 = f_2(x, y)$ gives the intersection of two lines. For a fixed $f_2(x, y)$, half of the scalar multiples of the right hand side of this equation give the intersection of two

$\mathbb{F}_q$-rational lines and half give the intersection of two Galois-conjugate lines. This shows that the quadratic residue weight enumerator is given by

$$\begin{aligned}\mathrm{QR}_{C_{1,2}}(X,Y,Z) &= X^{q+1} + \frac{(q+1)q(q-1)}{2} X^2 Y^{\frac{q-1}{2}} Z^{\frac{q-1}{2}} \\ &+ \frac{(q-1)(q+1)}{2} X(Y^q + Z^q) + \frac{(q-1)^2 q}{2} Y^{\frac{q+1}{2}} Z^{\frac{q+1}{2}}.\end{aligned}$$

The minimum weight codewords of ${C_{1,2}}^{\perp}$ have weight 4 and the MacWilliams theorem for this enumerator shows how these four nonzero coordinates split up into nonzero squares and non-squares. In this case, the $(q-1)\binom{q+1}{4}$ dual codewords of weight 4 contribute

$$\frac{(q-1)^3 q(q+1)}{32} Y^2 Z^2 + \frac{(q-5)(q-1)^2 q(q+1)}{192} \left(Y^4 + Z^4\right),$$

to the quadratic residue weight enumerator of ${C_{1,2}}^{\perp}$ if $q \equiv 1 \pmod 4$ and contribute

$$\frac{(q-3)(q-1)^2 q(q+1)}{32} Y^2 Z^2 + \frac{(q-1)^2 q(q+1)^2}{192} \left(Y^4 + Z^4\right),$$

if $q \equiv 3 \pmod 4$.

We give the quadratic residue weight enumerator for the code of quadrics in $\mathbb{P}^n(\mathbb{F}_q)$, $\mathrm{QR}_{C_{n,2}}(X,Y,Z)$, in Chapter 3. We also apply the MacWilliams theorem for this weight enumerator to get information about the low-weight dual code coefficients.

We compute this quadratic residue weight enumerator for quartics on $\mathbb{P}^1(\mathbb{F}_q)$ in Chapter 3 and use it to analyze points on families of elliptic curves over finite fields. We will give a more refined version of a result of Schoof [**40**] that builds on work of Deuring and Waterhouse [**14, 52**]. Applying the MacWilliams theorem here leads to interesting questions about powers of traces of elliptic curves over finite fields that are related to previous results of Birch [**3**].

The largest part of this thesis is spent studying del Pezzo surfaces of degree 2 over finite fields. In Chapter 2 we will review the theory of del Pezzo surfaces over

$\mathbb{F}_q$. We focus on the degree 2 case but also introduce the necessary background to give a thorough sketch of Elkies' results for cubic surfaces, and to set up the situation for del Pezzo surfaces of degree 4, which we return to in Chapter 6. We explain why codes coming from del Pezzo surfaces are amenable to this type of coding theoretic analysis.

We sketch enough of the theory to state our main result for del Pezzo surfaces of degree 2. Throughout this thesis we will suppose that the characteristic of $\mathbb{F}_q$ is not 2 or 3. In future work we hope to remove this restriction. The anti-canonical model of a del Pezzo surface of degree 2 is the double cover of $\mathbb{P}^2(\mathbb{F}_q)$ branched over a plane quartic curve. More concretely, we can describe such a surface as the zero locus of $w^2 = f_4(x, y, z)$ where $f_4(x, y, z)$ is a homogeneous quartic on $\mathbb{P}^2(\mathbb{F}_q)$. We will study this variety as a homogeneous quartic in the weighted projective space $\mathbb{P}(2, 1, 1, 1)$, where w has weight 2 and x, y, z each have weight 1.

There is a 15-dimensional space of such quartics. We consider the 16-dimensional code given by $\alpha w^2 = f_4(x, y, z)$. When $\alpha = 0$ the variety cut out by such an equation is a cone over the plane quartic $f_4(x, y, z) = 0$. When $\alpha \neq 0$ many quartics give rise to smooth or singular del Pezzo surfaces, but some, for example a quartic that is the fourth power of a linear form, lead to more singular varieties. We can count these singular cases using the combinatorics of $\mathbb{P}^2(\mathbb{F}_q)$. When $f_4(x, y, z)$ gives four coincident lines, the resulting variety is a cone over a genus one curve, which we can understand using the methods of Chapter 3. Removing these cases gives the following main result.

Theorem 3. *The following table lists, for each $T \in [0, 7]$, the number of quartics $f_4(x, y, z)$ with at most simple singularities such that $w^2 = f_4(x, y, z)$ gives a codeword with $q^2 + q + 1 + Tq$ coordinates equal to 0. For $T \neq 0$ this also counts the number of quartics giving a codeword with $q^2 + q + 1 - Tq$ coordinates equal to 0. The number*

is given as a multiple of $|\mathrm{GL}_3(\mathbb{F}_q)|/2903040$.

T	$2903040/\lvert\mathrm{GL}_3(\mathbb{F}_q)\rvert$ *times the number of* $w^2 = f_4(x,y,z)$ *of weight* $q^3 - Tq - 1$
0	$\frac{2^6\cdot 3^3\cdot 653}{\lvert\mathrm{GL}_3(\mathbb{F}_q)\rvert}\left(q^{15} + \frac{4103}{15672}q^{14} - \frac{18773}{15672}q^{13} + \frac{10715}{3918}q^{12} - \frac{32417}{7836}q^{11} + \frac{173425}{15672}q^{10} - \frac{274399}{15672}q^9 + \frac{132299}{15672}q^8 + \frac{44407}{15672}q^7 - \frac{8167}{3918}q^6 - \frac{1302}{653}q^5 - \frac{66353}{5224}q^4 + \frac{82845}{5224}q^3 - \frac{1680}{653}q^2 + \frac{1680}{653}\right)$
1	$\frac{3\cdot 7\cdot 29\cdot 1187}{(q-1)(q+1)}\left(q^8 + \frac{24499}{34423}q^7 + \frac{67671}{34423}q^6 + \frac{10890}{34423}q^5 + \frac{213612}{34423}q^4 - \frac{324549}{34423}q^3 + \frac{500399}{34423}q^2 + \frac{358280}{34423}q - \frac{608745}{34423}\right)$
2	$2^7\cdot 7\cdot 13^2\left(q^6 + \frac{15415}{10816}q^5 + \frac{1025}{1352}q^4 + \frac{77035}{10816}q^3 - \frac{198671}{10816}q^2 + \frac{314675}{5408}q - \frac{653745}{10816}\right)$
3	$3^3\cdot 5\cdot 7\cdot 13\left(q^6 + \frac{31}{39}q^5 + \frac{70}{13}q^4 - \frac{1591}{39}q^3 + \frac{2446}{13}q^2 - \frac{6536}{13}q + \frac{6351}{13}\right)$
4	$2^5\cdot 3\cdot 7\left(q^6 + \frac{5}{8}q^5 - \frac{185}{4}q^4 + \frac{3095}{8}q^3 - \frac{15673}{8}q^2 + \frac{9695}{2}q - \frac{34965}{8}\right)$
5	$3^2\cdot 7(q-3)\left(q^5 - 12q^4 + 146q^3 - 1235q^2 + 4461q - 5185\right)$
6	$2\cdot 3^2\cdot 7(q-7)(q-5)(q-3)(q^2 - 9q + 15)$
7	$(q-7)(q-5)(q-3)(q^3 - 20q^2 + 119q - 175)$

This is the analogue of a result of Elkies for cubic surfaces [**20**]. This theorem has some interesting geometric consequences for small q. For example, for $q = 9, 11$, there is a unique del Pezzo surface with q^2+8q+1 $\mathbb{F}_q$-rational points up to automorphism, while for $q = 13$ there are two isomorphism classes of such surfaces. We also show that for q satisfying certain congruence conditions $w^2 = x^4+y^4+z^4$ gives a del Pezzo surface with the maximal number of rational points. We prove this theorem and discuss these types of consequences in Chapter 4.

This approach has the potential to be applied in several other settings. For example, in Chapter 6 we set up much of the necessary material to prove the analogue of this result for del Pezzo surfaces of degree 4.

We note that his project fits in with previous work on counting points on varieties over finite fields. For example, Li has studied del Pezzo surfaces of degree 1 and 2 that have few rational points over $\mathbb{F}_q$ for small q [**31**]. Codes from del Pezzo surfaces have

also been investigated by Tsfasman and Vlăduţ [**49**], and Boguslavsky [**4, 5**], although their work focuses more on finding the minimal weights of subcodes rather than determining weight enumerators. More generally, codes coming from the evaluation of polynomials include famous examples such as Goppa codes and Reed-Solomon codes. Codes coming from quadrics and from curves given as complete intersections have been studied previously, but again, the focus has been on determining minimal weights rather than weight enumerators [**46, 47, 50, 51**]. Finally, low-weight dual codewords of codes of this type have been studied by Couvreur [**13**], and Fontanari and Marcolla [**22**].

There is a large computational component to this thesis. Most of these computations were done in the computer algebra system Sage [**45**]. We also use the algebra system Magma in Chapter 4 to compute the automorphism groups of certain curves over finite fields [**6**].

CHAPTER 2

Del Pezzo Surfaces over Finite Fields

This chapter gives the necessary background for the weight enumerator calculation for del Pezzo surfaces of degree 2. We begin by giving several of the basic definitions in this area and reviewing the classical theory. We will also give a fairly detailed sketch of Elkies' results about the distribution of point counts for cubic surfaces [**20**]. At the end of this chapter we give an outline of the proof of Theorem 3, breaking it up into a combinatorial part, a part about elliptic curves over finite fields, and a rather intricate computation involving low-weight coefficients of the dual of two particular codes.

We will state a first goal for this section.

Proposition 4. *Suppose that $f_4(x, y, z) = 0$ defines a plane quartic that does not have non-isolated singularities and is not the union of four coincident lines. Then $w^2 = f_4(x, y, z)$ defines a homogeneous quartic in $\mathbb{P}(2, 1, 1, 1)$ with $q^2 + q + 1 + tq$ $\mathbb{F}_q$-rational points, for some integer $t \in [-7, 7]$.*

1. The Geometry of del Pezzo Surfaces

This section relies heavily on Chapter 8 of Dolgachev's book [**15**]. We begin with the classical definition of a del Pezzo surface. We recall that a surface in $\mathbb{P}^n$ is called *nondegenerate* if it is not contained in a proper linear subspace of $\mathbb{P}^n$.

Definition. *A* del Pezzo surface *is a nondegenerate irreducible surface of degree d in $\mathbb{P}^d$ that is not a cone and not isomorphic to a projection of a surface of degree d in $\mathbb{P}^{d+1}$.*

The more modern viewpoint is to define these surfaces in terms of the anti-canonical class $-K_S$.

Definition. *A* del Pezzo surface *is a nonsingular surface S with ample $-K_S$. A* weak del Pezzo surface *is a nonsingular surface with $-K_S$ nef and big.*

We recall that a divisor D is called nef*, or* numerically effective*, if for any irreducible curve C the intersection number $C \cdot D > 0$. If we only require $C \cdot D \geq 0$ then D is called* ample*. We say that D is* big *if its self-intersection is positive, $D^2 > 0$.*

We will refer to a singular surface that has minimal desingularization equal to a del Pezzo surface as a *singular del Pezzo surface*. The most natural invariant of a del Pezzo surface is its degree.

Definition. *The number $d := K_S^2$ is called the degree of a weak del Pezzo surface.*

It is not difficult to prove that a del Pezzo surface has degree at most 9. In this thesis we focus on the particular case of del Pezzo surfaces of degree 2, but also discuss Elkies' work on del Pezzo surfaces of degree 3 (cubic surfaces) and will mention del Pezzo surfaces of degree 4 in Chapter 6. Del Pezzo surfaces of different degrees have much in common, but each degree has its own flavor.

The definition of a weak del Pezzo surface limits the types of curves it can contain. The curves that do appear play a special role in the study of rational points of del Pezzo surfaces over finite fields.

Proposition 5. *Let S be a weak del Pezzo surface. Then any irreducible reduced curve C on S with negative self-intersection satisfies $C \cdot C = -1$ or -2.*

This is Lemma 8.1.13 of [**15**]. We say that such a C is a (-1)-curve, or a (-2)-curve, respectively. The divisor classes of these curves play an important role in studying the Picard group $\mathrm{Pic}(S)$ of S, because they arise from blow-ups.

Del Pezzo surfaces have only rational double points as singularities. These singularities are related to the presence of (-2)-curves on the minimal desingularization of the surface. We will not need to study these singularities in detail. For more information see [**15**].

Proposition 6.

(1) A del Pezzo surface S has only rational double points as singularities.

(2) A smooth del Pezzo surface S does not contain any (-2)-curves. Let S be a singular del Pezzo surface and $\pi : \overline{S} \to S$ a minimal desingularization. Then $\overline{S}$ is a weak del Pezzo surface and the inverse image of the singular points of S is exactly the collection of (-2)-curves on $\overline{S}$.

The first part of this statement is Theorem 8.1.11 in [**15**]. The second part follows from Theorem 2.4.4 of [**32**].

We see that S has a rational double point if and only if its minimal desingularization $\overline{S}$ has a (-2)-curve. We are primarily concerned with rational points not on del Pezzo surfaces S, but on the anti-canonical model of S, which we define below. For example, we do not study rational points on del Pezzo surfaces of degree 3, but on models of such surfaces as cubic hypersurfaces in $\mathbb{P}^3(\mathbb{F}_q)$, and do not study points on del Pezzo surfaces of degree 2, but on double covers of $\mathbb{P}^2(\mathbb{F}_q)$ branched over a plane quartic. The rational double points on S, the (-2)-curves on $\overline{S}$, and singular points on these models, for example on the cubic surface or quartic curve, are all closely related.

We would like to give a concrete way to produce all del Pezzo surfaces of given degree d over a fixed finite field $\mathbb{F}_q$. We can do this by describing these surfaces as the blow-up of $\mathbb{P}^2$ at $9-d$ points. We first recall that a blow-up of a variety X at a point x is a variety $\overline{X}$ along with a morphism $\pi : \overline{X} \to X$. The inverse image of x is called the exceptional divisor E of the blow-up, and π is an isomorphism outside

of E. A point $x' \in \overline{X}$ is *infinitely near* to x if it lies in the support of E. Given a collection of points $\{x_1, \ldots, x_n\}$, the point x_i is *proper* if no x_j with $j \neq i$ is infinitely near to x_i.

For the blow-up $\mathbb{P}^2$ at N points, we consider a composition of birational morphisms

$$\pi : \ S = S_k \stackrel{\pi_k}{\to} S_{k-1} \stackrel{\pi_{k-1}}{\longrightarrow} \cdots \stackrel{\pi_2}{\to} S_1 \stackrel{\pi_1}{\to} \mathbb{P}^2,$$

where each $\pi_i : \ S_i \to S_{i-1}$ is the blow-up of a point x_i in S_{i-1}. If all of these points are proper, then they are in $\mathbb{P}^2$, but can also consider the blow-up of $\mathbb{P}^2$ at infinitely near points.

We note that F_2 is the Hirzebruch surface, a minimal ruled surface. The following result is Corollary 8.1.17 of [**15**].

Theorem 7. *Let S be a weak del Pezzo surface. Then either $S \cong \mathbb{P}^1 \times \mathbb{P}^1$, or $S \cong F_2$, or S is obtained from $\mathbb{P}^2$ by blowing up $N \leq 8$ points. If S is a nonsingular del Pezzo surface, then the case $S \cong F_2$ does not occur.*

It is not the case that blowing up any collection of $N \leq 8$ points leads to a weak del Pezzo surface. We give exactly the conditions that yield weak del Pezzo surfaces.

Proposition 8. *Let $\eta = \{x_1, \ldots, x_r\}$ be a collection of points in $\mathbb{P}^2$, possibly infinitely near, and S_η be the blow-up of these points. Then S_η is a weak del Pezzo surface if and only if each of the following conditions holds:*

(1) $r \leq 8$;

(2) the Enriques diagram of η is the disjoint union of chains;

(3) $|\mathcal{O}_{\mathbb{P}^2}(1) - \eta'| = \emptyset$ for any $\eta' \subset \eta$ consisting of four points;

(4) $|\mathcal{O}_{\mathbb{P}^2}(2) - \eta'| = \emptyset$ for any $\eta' \subset \eta$ consisting of seven points.

This is Corollary 8.1.24 of [**15**]. We will not define the Enriques diagram here because it is not needed in what follows. See Section 7.3.2 of [**15**] for details.

Points satisfying these four conditions are said to be in *almost general position*. We next give the analogous definition for general position and the analogue of the above result for del Pezzo surfaces.

Definition. *We say that a collection of points is in* general position *if each of the following conditions holds:*

(1) all points are proper points;

(2) no three points are on a line;

(3) no six points are on a conic.

Proposition 9. *The blow-up of $N \leq 7$ points in $\mathbb{P}^2$ is a smooth del Pezzo surface if and only if the points are in general position.*

The blow-up of 8 points in $\mathbb{P}^2$ is a smooth del Pezzo surface if and only if it satisfies these conditions and also no cubic passes through these 8 points with one of the points being a singular point.

The first part of this result follows from Proposition 8. The second part is Proposition 8.1.25 of [**15**].

Next we describe how this modern notion of del Pezzo surface relates to the classical definition that began this section. This connection comes from the anti-canonical map. The following result, Theorem 8.3.2 of [**15**], explains why we study the particular models of curves mentioned above, cubic surfaces and double covers of $\mathbb{P}^2$ branched over plane quartics. This also provides a concrete link between rational double points of a del Pezzo surface and the (-2)-curves of its minimal desingularization.

Theorem 10. *Let S be a weak del Pezzo surface of degree d and let $\mathcal{R}$ be the union of (-2)-curves on S. Then we have the following:*

(1) $|-K_S|$ has no fixed part.

(2) If $d > 1$, then $|-K_S|$ has no base points.

(3) *If $d > 2$, then $|-K_S|$ defines a regular map ϕ to $\mathbb{P}^d$ that is an isomorphism outside of $\mathcal{R}$. The image surface $\overline{S}$ is a del Pezzo surface of degree d in $\mathbb{P}^d$. The image of each connected component of $\mathcal{R}$ is a rational double point of $\phi(S)$.*

(4) *If $d = 2$, then $|-K_S|$ defines a regular map $\phi : S \to \mathbb{P}^2$. It factors as a birational morphism $f : S \to \overline{S}$ onto a normal surface and a finite map $\pi : \overline{S} \to \mathbb{P}^2$ of degree 2 branched along a not necessarily irreducible curve B of degree 4. The image of each connected component of $\mathcal{R}$ is a rational double point of $\overline{S}$. The curve B is either nonsingular or has only simple singularities.*

(5) *If $d = 1$, then $|-2K_S|$ defines a regular map $\phi : S \to \mathbb{P}^3$. It factors as a birational morphism $f : S \to \overline{S}$ onto a normal surface and a finite map $\pi : \overline{S} \to Q \subset \mathbb{P}^3$ of degree 2, where Q is a quadric cone. The morphism π is branched along a curve B of degree 6 cut out on Q by a cubic surface. The image of each connected component of $\mathcal{R}$ under f is a rational double point of $\overline{S}$. The curve B is either nonsingular or has only simple singularities.*

We emphasize a certain difficulty in studying del Pezzo surfaces in terms of blow-ups. We are interested in anti-canonical models of del Pezzo surfaces over $\mathbb{F}_q$, that is, the coefficients of the defining equation are in $\mathbb{F}_q$. This does not mean that a del Pezzo surface S of degree d is the blow-up of $9 - d$ points of $\mathbb{P}^2$ where the maps are considered over $\mathbb{F}_q$, even if we do not require the individual points to be $\mathbb{F}_q$-rational points. We consider the blow-ups to be defined over the algebraic closure $\overline{\mathbb{F}}_q$. This gives an equation for the anti-canonical model. We are only interested in choices of coordinates where the defining coefficients are in $\mathbb{F}_q$. We then study the $\mathbb{F}_q$-rational solutions to this equation. It is clear that for a surface defined over the algebraic closure there can be many choices of coordinates for the anti-canonical model that give an equation defined over $\mathbb{F}_q$ but with different numbers of $\mathbb{F}_q$-rational solutions.

We now focus on the case $d = 2$. We will study the $2:1$ map π for del Pezzo surfaces of degree 2 in detail in Chapter 4. We recall that a simple singularity is one that is isolated and has no moduli. More formally, a simple singularity is characterized by the property that there are only finitely many isomorphism classes of indecomposable torsion-free modules over its local ring [**15**]. We note that the quartic given by four coincident lines has a singularity that is not simple, but 'simple elliptic' [**9**]. This implies that the double cover of $\mathbb{P}^2$ branched along a quartic that has non-isolated singular points does not give a weak del Pezzo surface, nor does the double cover branched along the union of four coincident lines. For a linear system L, let $L^\vee$ denote the dual linear system. The following result is Proposition 6.3.9 in [**15**].

Proposition 11. *Let $\mathcal{P} = \{p_1, \ldots, p_7\}$ be a set of seven distinct points in $\mathbb{P}^2$ in general position. Let L be the linear system of cubic curves through these points. The rational map $L \to L^\vee$ given by the linear system L is of degree 2. It extends to a regular degree 2 finite map $\pi : X \to L^\vee \cong \mathbb{P}^2$, where X is the blow-up of the set $\mathcal{P}$. The branch curve C is a nonsingular plane quartic in $L^\vee$. The ramification curve R is the proper transform of a curve $B \subseteq L$ of degree 6 with double points at each p_i.*

Conversely, given a nonsingular plane quartic C, the double cover of $\mathbb{P}^2$ ramified over C is a nonsingular surface isomorphic to the blow-up of 7 points $p_1, \ldots, p_7$ in general position.

In this thesis we study counts for rational points on del Pezzo surfaces of degree 2 in terms of rational point counts for double covers of $\mathbb{P}^2$ branched along plane quartics. Certain plane quartics do not lead to del Pezzo surfaces, but to varieties with more complicated singularities, cones over genus 1 curves for example, but quartics with at most simple singularities will be the most interesting situation.

2. The Picard Group of a Weak del Pezzo Surface

In order to understand rational points on del Pezzo surfaces we will study Picard groups of these surfaces in detail. A theorem of Weil, which we state below, lets us write the number of $\mathbb{F}_q$-rational points on a del Pezzo surface in terms of the trace of the Frobenius endomorphism acting on its Picard group. In fact, this is the key property that makes our method of counting points work in this case, but not for more general surfaces. For example, our methods will not extend easily to study rational points on cubic surfaces in $\mathbb{P}^4$ because these point counts cannot be understood as easily in terms of $\mathrm{Pic}(S)$.

We can give a very explicit description of the Picard group of a del Pezzo surface because such a surface arises as a blow-up of $\mathbb{P}^2$. The following result describes the Picard group of a blow-up. This is Theorem 2.2.2 of Loughran's thesis [**32**]. The proof is assembled from several propositions in Hartshorne [**24**].

Proposition 12. *Let X be a smooth projective surface, and let $\pi : \overline{X} \to X$ be the blow-up of X at a point x with exceptional divisor E. Then $\overline{X}$ is a smooth projective surface and $K_{\overline{X}} = \pi^* K_X + E$. Moreover the natural map*

$$\begin{aligned} \mathrm{Pic}(X) \oplus \mathbb{Z} &\to \mathrm{Pic}(\overline{X}) \\ (D, n) &\to \pi^*(D) + nE, \end{aligned}$$

is an isomorphism. The following facts completely determine the intersection behavior of divisors of X.

(1) $\pi^*(D_1) \cdot \pi^*(D_2) = D_1 \cdot D_2$ for any two divisors D_1, D_2 on X.

(2) $\pi^*(D) \cdot E = 0$ for any divisor D on X.

(3) E is a (-1)-curve.

(4) $\pi^*(D) = \overline{D} + rE$ where D is any effective divisor on X with multiplicity r through x. In particular $\overline{D}^2 = D^2 - r$.

In fact, any (-1)-curve on X arises as the exceptional divisor of a blow-up of some surface at a smooth rational point.

The following definition gives an explicit way to write down a basis for the Picard group of a weak del Pezzo surface [**15**].

Definition. *A* blowing-down structure *on a weak del Pezzo surface S is a composition of birational morphisms*

$$\pi : \ S = S_N \stackrel{\pi_N}{\to} S_{N-1} \stackrel{\pi_{N-1}}{\longrightarrow} \cdots \stackrel{\pi_2}{\to} S_1 \stackrel{\pi_1}{\to} \mathbb{P}^2,$$

where each $\pi_i : \ S_i \to S_{i-1}$ is the blow-up of a point x_i.

Set

$$\pi_{ki} := \pi_{i+1} \circ \cdots \circ \pi_k : \ S_k \to S_i, \ k > i.$$

Let $E_i = \pi_i^{-1}(x_i)$ and $\mathcal{E} = \pi_{Ni}^*(E_i)$. The divisors $\mathcal{E}_i$ are called the exceptional configurations *of the birational morphism $\pi : \ S \to \mathbb{P}^2$.*

Proposition 13. *A blowing-down structure on a del Pezzo surface S gives a basis $(H, e_1, \ldots, e_N)$ in $\mathrm{Pic}(S)$, where H is the class of the full preimage of a line and e_i is the class of the exceptional configuration $\mathcal{E}_i$ defined by the point x_i.*

The canonical class is represented by

$$k_N = -3H + e_1 + \cdots + e_N$$

in this basis.

We call such a basis a *geometric basis*. See Section 7.5.1 of [**15**] for a proof. A geometric basis gives a way to identify the Picard group with a well-known class of lattices.

Proposition 14. *A blowing-down structure defines an isomorphism of free abelian groups $\phi : \ \mathbb{Z}^{N+1} \to \mathrm{Pic}(S)$, such that $\phi(k_N) = K_S$.*

The orthogonal complement of the lattice spanned by k_N is isomorphic to the negative definite lattice E_N. A basis for E_N is given by

$$H - e_1 - e_2 - e_3, e_1 - e_2, e_2 - e_3, \ldots, e_{N-1} - e_N.$$

Again, see Chapter 7 of [**15**] for a proof.

We note that many sources consider E_N to be a positive definite lattice, so would call the lattice in this proposition $E_N\langle -1\rangle$, that is, E_N with the inner product scaled by -1. We also define two other classes of lattices that occur as sublattices of E_N.

Definition. *For $N \geq 3$, D_N is the checkerboard lattice*

$$\left\{(x_1, \ldots, x_N) \in \mathbb{Z}^N : \ x_1 + \cdots + x_N \equiv 0 \pmod 2\right\}.$$

For $N \geq 1$, A_N is defined by

$$\left\{(x_0, \ldots, x_N) \in \mathbb{Z}^{N+1} : \ x_0 + x_1 + \cdots + x_N = 0\right\}.$$

This is an n-dimensional lattice embedded in $\mathbb{Z}^{n+1}$ as the integer points of a hyperplane. It is possible, although a little less nice, to write A_n as a sublattice of $\mathbb{R}^n$.

We also recall the standard form for E_8. Let

$$E_8 = \left\{(x_1, \ldots, x_8) : \ \text{all } x_i \in \mathbb{Z} \text{ or all } x_i \in \mathbb{Z} + \frac{1}{2}, \ \sum_{i=1}^{8} x_i \equiv 0 \pmod 2\right\}.$$

We can define E_N for $N < 8$ in terms of orthogonal complements of vectors of E_8.

We note that $A_3 \cong D_3$ and that $E_3 \cong A_1 \oplus A_2$, that $E_4 \cong A_4$, and that $E_5 \cong D_5$, where these E_N are positive definite. From this definition it is not clear that E_8 is a lattice at all since it is written as the union of vectors in a copy of D_8 and a shifted copy of D_8, but one can see that it is by writing down a basis for it. Our interest in these lattices comes from their occurrence as lattices generated by (-2)-curves on

weak del Pezzo surfaces, but we point out that they play a key role in many other areas of mathematics. For more details see [**12**].

Given a lattice $L \subset \mathbb{R}^N$, there are two important related lattices we derive from it. We note that a lattice in $\mathbb{R}^N$ comes equipped with an inner product.

Definition. *Suppose L is a sublattice of M. We define the* orthogonal complement *of L in M by*

$$L^{\perp} = \{y \in M : \ x \cdot y = 0 \ \forall x \in L\}.$$

The dual lattice *of L is*

$$L^* = \{y \in L \otimes \mathbb{R} : \ x \cdot y \in \mathbb{Z} \ \forall x \in L\}.$$

A lattice L is called *integral* if $\langle x, y \rangle \in \mathbb{Z}$ for all $x, y \in L$. It is not difficult to show that if L is integral then

$$L \subset L^* \subseteq \frac{1}{\det(L)} L,$$

where $\det(L)$ is the square of the determinant of a generator matrix of L. It will be useful for us to consider the group L^*/L. For example, A_N^*/A_N is a cyclic group of order $N+1$, and E_7^*/E_7 has order 2. In Chapter 4 we will need to consider $A_1 \subset E_7$ and its orthogonal complement inside this lattice, which is a copy of D_6 [**12**].

We need a few more definitions in order to understand the (-2)-curves of a weak del Pezzo surface in terms of lattices. We now return to the negative definite version of E_N along with the basis we described above.

Definition. *A vector $\alpha \in E_N$ is called a* root *if $\alpha^2 = -2$. Suppose that $N \in [3, 8]$. An ordered set B of roots $\{\beta_1 \ldots, \beta_r\}$ is called a* root basis *if they are linearly independent over $\mathbb{Q}$ and $\beta_i \cdot \beta_j \geq 0$. A root basis is called* irreducible *if it is not equal to the union of non-empty subsets B_1 and B_2 such that $\beta_i \cdot \beta_j = 0$ if $\beta_i \in B_1$ and $\beta_j \in B_2$. The symmetric $r \times t$ matrix C with (i, j) entry $\beta_i \cdot \beta_j$ is called the* Cartan matrix *of this*

root basis. A lattice with a quadratic form defined by a Cartan matrix is called a root lattice. *In this setting, the quadratic form will be negative definite. A sublattice $R \subset E_N$ isomorphic to a root lattice is called a* root sublattice.

A canonical root basis *in E_N is a root basis with Cartan matrix equal to the one for the basis given above in terms of $H, e_1, \ldots, e_N$, and with Coxeter-Dynkin diagram equal to the standard one for E_N.*

We will not define a Coxeter-Dynkin diagram here, but note that it is a graph given by considering inner products between basis vectors. See Section 8.2.3 of [**15**] for details. The first part of the following result is Proposition 8.2.10 of [**15**]. The second is a classical result independently due to Borel and de Siebenthal, and Dynkin. This is also explained in Section 8.2.3 of [**15**].

Proposition 15. *The Cartan matrix C of an irreducible root basis in E_N is equal to an irreducible Cartan matrix of type A_r, D_r, E_r with $r \leq N$.*

Every root sublattice of E_N is isomorphic to the orthogonal sum of root lattices with irreducible Cartan matrices. These can be classified in terms of root bases.

Our goal in this discussion has been to understand singular del Pezzo surfaces, or equivalently (-2)-curves on weak del Pezzo surfaces, in terms of certain root lattices. The following result is Proposition 8.2.25 of [**15**].

Proposition 16. *Let S be a weak del Pezzo surface of degree $d = 9 - N$. The number r of (-2)-curves on S is less than or equal to N. The sublattice $\mathcal{R}_S$ of* $\mathrm{Pic}(S)$ *generated by these (-2)-curves is a root lattice of rank r.*

We introduce one more definition in order to clarify the connection between singular points of del Pezzo surfaces and (-2)-curves on weak del Pezzo surfaces.

Definition. *A* Dynkin curve *is a reduced connected curve R on a projective nonsingular surface X such that its irreducible components R_i are (-2)-curves and the*

matrix $(R_i \cdot R_j)$ *is a Cartan matrix. The* type *of a Dynkin curve is the type of the corresponding root system.*

Rational double points can be described in terms of these root systems. This gives the direct link between singularities of del Pezzo surfaces and the sublattice of E_N generated by the classes of (-2)-curves of its minimal desingularization.

Theorem 17. *A rational double point is locally analytically isomorphic to one of the following singularities:*

$$\begin{aligned}
A_n: &\quad z^2 + x^2 + y^{n+1} = 0, \quad n \geq 1,\\
D_n: &\quad z^2 + y(x^2 + y^{n-2}) = 0, \quad n \geq 4,\\
E_6: &\quad z^2 + x^3 + y^4 = 0,\\
E_7: &\quad z^2 + x^3 + xy^3 = 0,\\
E_8: &\quad z^2 + x^3 + y^5 = 0.
\end{aligned}$$

The corresponding Dynkin curve is of respective type A_N, D_N, E_N.

There is a correspondence between these surface singularities and the simple singularities of plane curves as classified by du Val. We will focus on the case of del Pezzo surfaces of degree 2. This next result follows from the discussion in Section 8.7.1 of [**15**].

Theorem 18. *Let* S *be a singular del Pezzo surface and* $\overline{S}$ *the weak del Pezzo surface that is its minimal desingularization. This resolution of singularities composed with the anti-canonical map gives a double cover*

$$\pi: \ \overline{S} \to S \to \mathbb{P}^2,$$

branched over a plane quartic B. The singularities of B coincide with the singularities of S. Let x be a singular point of B. Then $\pi^*(x)$ is a Dynkin curve on $\overline{S}$ with the same singularity type.

It is instructive to look at this result together with Proposition 11. Now that we have given a thorough discussion of (-2)-curves and their relation to singular points, we turn to the connection between (-1)-curves and lines.

Definition. *A vector in $\mathbb{Z}^{N+1} \cong \mathrm{Pic}(S)$ is called exceptional is $k_N \cdot v = v \cdot v = -1$. An exceptional curve is a (-1)-curve on S associated to an exceptional vector.*

Let S be a weak del Pezzo surface. Let $\phi : \mathbb{Z}^{N+1} \to \mathrm{Pic}(S)$ come from a geometric basis of $\mathrm{Pic}(S)$. We recall that such a basis is equivalent to a blowing-down structure of S.

In order to explain the connection between (-1)-curves on a weak del Pezzo surface and lines on the anti-canonical model we briefly discuss the Weyl group.

Definition. *Let $\beta = (\beta_1, \ldots, \beta_N)$ be a canonical root basis for E_N. We define the* Weyl group of E_N, *denoted $W(E_N)$, to be the group generated by the reflections r_{β_i}.*

Let S be a weak del Pezzo surface and $(H, e_1, \ldots, e_N)$ be a geometric basis for $\mathrm{Pic}(S)$. *We let $W(S)$ be the group generated by reflections with respect to the roots of the orthogonal complement of k_N. We also define $W(S)^n$ to be the subgroup of $W(S)$ generated by reflections with respect to (-2)-curves.*

The following result is Proposition 8.2.34 in [**15**].

Proposition 19. *Let $\phi : W(S) \to W(E_N)$ be an isomorphism of groups give by a geometric basis of* $\mathrm{Pic}(S)$. *There is a natural bijection*

$$(-1)\text{-curves on } S \leftrightarrow W(S)^n/\phi^{-1}(\mathrm{Exc}_N),$$

where Exc_N *denotes the set of exceptional vectors in $\mathbb{Z}^{N+1}$.*

Weyl groups play an important role in Chapter 4 because of their relationship to blowing-down structures for a weak del Pezzo surface.

Proposition 20. *The group $W(E_N)$ acts simply transitively on canonical root bases of E_N.*

This is Corollary 8.2.15 in [**15**]. This follows from studying the stabilizer of the canonical class k_N. This gives a way to compute the orders of the Weyl groups of the E_N lattices.

Proposition 21. *The orders of the Weyl groups $W(E_N)$ are given by the following table:*

N	3	4	5	6	7	8
$\#W(E_N)$	$2^2 \cdot 3$	$5!$	$2^4 \cdot 5!$	$2^3 \cdot 3^2 \cdot 6!$	$2^6 \cdot 3^2 \cdot 7!$	$2^7 \cdot 3^3 \cdot 5 \cdot 8!$

.

This is a well-known result about the E_N lattices. It is given as Corollary 8.2.20 in [**15**] where it is proven by relating the order of $W(E_N)$ to the order of $W(E_{N-1})$ by studying the stabilizer of a single vector.

We will give a general summary of the kinds of exceptional curves that occur for smooth del Pezzo surfaces. This is Theorem 26.2 in Manin's book [**35**].

Theorem 22. *Let S be a smooth del Pezzo surface of positive degree d satisfying $2 \leq d \leq 7$ and let $\pi : S \to \mathbb{P}^2$ be its representation as the blow-up of the plane at $N = 9 - d$ points $x_1, \ldots, x_N$. Then the following assertions hold:*

(1) The map that takes an exceptional curve to its divisor class in $\mathrm{Pic}(S)$ *gives a one-to-one correspondence between exceptional curves of S and classes D in* $\mathrm{Pic}(S)$ *such that $D \cdot K_S = D^2 = -1$. These classes generate* $\mathrm{Pic}(S)$.

(2) The image $\pi(D)$ in $\mathbb{P}^2$ of a (-1)-curve of S is one of the following types:

(a) one of the points x_i;

(b) a line passing through two of the points x_i;

(c) a conic passing through five of the points x_i;

(d) a cubic passing through seven of the points x_i such that one of them is a double point;

(3) The number of lines of S is given by the following table:

N	3	4	5	6	7
# Lines	6	10	16	27	56

.

We have omitted the statement of this result for del Pezzo surfaces of degree 1 because it is more complicated and we will not need it in the rest of this thesis. We note that for $d \geq 3$ only the first three types of images occur. We also note that one can give a similar statement for exceptional curves on a singular del Pezzo surface, although the number of such curves changes depending on the singularity type.

We now consider lines of del Pezzo surfaces of degree 2. For a smooth surface S of degree 2 there are 56 lines. The anti-canonical model of S is the double cover of $\mathbb{P}^2$ branched over a plane quartic curve B. When S is singular the branch quartic is singular as well and the types of these singularities coincide. We study the (-1)-curves in terms of bitangents of B.

The 56 lines come in 28 pairs that correspond to the 28 bitangents of B as follows. Let $\overline{S}$ be the minimal desingularization of the singular del Pezzo surface S and $\pi : \overline{S} \to \mathbb{P}^2$ be the composition of this desingularization with the $2:1$ map to $\mathbb{P}^2$. The restriction of ϕ to a (-1)-curve E has image equal to a line l in $\mathbb{P}^2$. The preimage of l is a divisor $D = E' + R$, where E' is a (-1)-curve on $\overline{S}$ and R is the union of (-2)-curves. From this we can see that l is either tangent to C at two nonsingular points, tangent to B at one nonsingular point and passes through a singular point, or is a component of B. We have seen that we can determine the singular lattice generated by (-2)-curves of $\overline{S}$ by classifying the singularities of B. For an extensive discussion of the role that bitangents play in the theory of plane quartics and a more

detailed discussion of the correspondence between the 28 bitangents and the 56 lines of a del Pezzo surface of degree 2 see Chapter 6 and Section 8.7.1 of [**15**].

There is a special kind of set of bitangents of a quartic curve called an Aronhold set, or Aronhold seven. We note that a blowing-down structure of a smooth del Pezzo surface S corresponds to an Aronhold set of seven bitangents. An Aronhold set of bitangents is equivalent to a set of seven (-1)-curves $E_1, \ldots, E_7$ such that $E_i \cdot E_j = 0$ for $i \neq j$. For a definition of an Aronhold set in terms of theta characteristics see Section 6.1.2 [**15**].

3. Points on del Pezzo Surfaces over Finite Fields

Our next goal is to understand the number of rational points of a del Pezzo surface S defined over $\mathbb{F}_q$ in terms of the Galois structure of its Picard group $\mathrm{Pic}(S)$. Over $\mathbb{F}_q$ we have the Frobenius endomorphism $\varphi : \mathbb{P}^n(\bar{\mathbb{F}}_q) \to \mathbb{P}^n(\bar{\mathbb{F}}_q)$, which sends a point $[x_0 : x_1 : \cdots : x_n]$ to $[x_0^q : x_1^q : \cdots : x_n^q]$, taking the qth power of each coordinate. The $\mathbb{F}_q$-points of $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ are exactly those points fixed by φ. A major idea of modern arithmetic algebraic geometry is to study these questions about $\mathbb{F}_q$-points of varieties using various fixed-point theorems from algebraic topology. For example, there is the Grothendieck trace formula that describes the number of fixed points of the Frobenius morphism acting on a variety X over $\mathbb{F}_q$ in terms of the trace of its action on certain étale cohomology groups.

In this thesis we are able to avoid the intricacies of the theory of étale cohomology since the surfaces we study will mostly be birationally trivial, that is, birational to $\mathbb{P}^2$ over $\bar{\mathbb{F}}_q$. In this case, these groups are much easier to understand. A result of Weil implies that we can understand the fixed points of Frobenius by understanding its action on the Picard group of S [**35**].

Theorem 23 (Weil)**.** *Let S be a surface defined over a finite field $\mathbb{F}_q$. If $S \otimes \overline{\mathbb{F}}_q$ is birationally trivial, then*

$$\#S(\mathbb{F}_q) = q^2 + q\mathrm{Tr}(\varphi^*) + 1,$$

where φ denotes the Frobenius endomorphism and $\mathrm{Tr}(\varphi^*)$ denotes the trace of φ in the representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on $\mathrm{Pic}(S \otimes \overline{\mathbb{F}}_q)$.

We see that this theorem applies to weak del Pezzo surfaces. However, our real goal is to count rational points on anti-canonical models of del Pezzo surfaces. We will focus here on surfaces of degree 2, but much of what we say holds more generally.

Let S be a singular del Pezzo surface with minimal desingularization $\overline{S}$ and $\pi : \overline{S} \to \mathbb{P}^2$ be the composition of this desingularization with the anti-canonical map. The theorem above allows us to count points on $\overline{S}$, but this does not necessarily coincide with rational points on the image of π. This is because the (-2)-curves of $\mathrm{Pic}(\overline{S})$ are sent to the singular points of the anti-canonical model. This can change the counts for rational points.

Proposition 24. *Let S be a del Pezzo surface, possibly singular, and $\overline{S}$ the weak del Pezzo surface that is its minimal desingularization. Let $\mathcal{R} \subset E_7$ be the root sublattice generated by (-2)-curves of $\overline{S}$. Then the number of $\mathbb{F}_q$-rational points of the anti-canonical model of S is given by $q^2 + q + 1 + qt$, where*

$$t = \mathrm{Tr}(\varphi|_{E_7}) - \mathrm{Tr}(\varphi|_{\mathcal{R}}) = \mathrm{Tr}(\varphi|_{\mathcal{R}^\perp}).$$

Proof. Every (-2)-curve of $\overline{S}$ is orthogonal to the canonical class K_S, so $\mathcal{R}$ is a sublattice of E_7. We can extend a $\mathbb{Q}$-basis $\{\beta_1, \ldots, \beta_r\}$ of $\mathcal{R}$ to a basis of E_7. We consider $\mathcal{R}^\perp \subset E_7$. Even though E_7 does not have to be a direct sum of $\mathcal{R}$ and $\mathcal{R}^\perp$ we can choose a $\mathbb{Q}$-basis for E_7, $\{\beta_1, \ldots, \beta_r, \beta_{r+1}, \ldots, \beta_7\}$, where the first r elements form a $\mathbb{Q}$-basis for $\mathcal{R}$, and the last $7 - r$ form a $\mathbb{Q}$-basis for $\mathcal{R}^\perp$. We note that $\mathrm{Pic}(\overline{S})$

is generated by classes of the (-1)-curves of $\overline{S}$ and that φ permutes these curves. Therefore,

$$\mathrm{Tr}(\varphi|_{E_7}) = \mathrm{Tr}(\varphi|_{\mathcal{R}}) + \mathrm{Tr}(\varphi|_{\mathcal{R}^\perp}).$$

Combining this observation with Theorem 23 completes the proof. □

We note that the trace of Frobenius acting on a sublattice of E_7 is bounded in absolute value by the dimension of the lattice. Let r be $\dim(\mathcal{R})$. We have

$$\mathrm{Tr}(\varphi|_{\mathcal{R}^\perp}) = \mathrm{Tr}(\varphi|_{E_7}) - \mathrm{Tr}(\varphi|_{\mathcal{R}}),$$

and conclude that $|\mathrm{Tr}(\varphi|_{\mathcal{R}^\perp})| \leq 7 - r$. We will use this fact in Chapter 4. By a slight abuse of notation we will often refer to a del Pezzo surface whose anti-canonical model has $q^2 + q + 1 + tq$ points as a del Pezzo surface of trace t.

This result makes it much easier to study rational points on del Pezzo surfaces over finite fields. We can explicitly write down generators of the Picard group of S in terms of a geometric basis, or a blowing-down structure of S. We can determine the sublattice of $\mathrm{Pic}(S)$ generated by (-2)-curves by studying the singularities of the branch quartic given by the anti-canonical model. It is clear that Frobenius preserves the intersection theory of $\mathrm{Pic}(S)$. Therefore, it sends a canonical root basis to a canonical root basis. By Proposition 20 the permutation of (-1)-curves of S is given by an element of the Weyl group of S. For a weak del Pezzo surface, we see that $\mathrm{Tr}(\varphi|_{E_7}) = \mathrm{Tr}(g)$, for some element $g \in W(E_7)$.

The Weyl group of a del Pezzo surface is finite, so we may tabulate the distribution of $\mathrm{Tr}(g)$ as g varies. Checking the character tables of $W(E_6)$ and $W(E_7)$ gives the following results.

Proposition 25. *Let $\pi \in W(E_6)$, the Weyl group of E_6. Then $\mathrm{Tr}(\pi) \in [-3, 6] \setminus \{5\}$. The number of elements of $W(E_6)$ with each trace value is given by the following*

table:

Trace	-3	-2	-1	0	1	2	3	4	6
$\#W(E_6)$	80	3465	11664	20820	13104	24300	120	36	1

.

Let $\pi \in W(E_7)$, the Weyl group of E_7. Then $\mathrm{Tr}(\pi) \in [-7,7] \setminus \{-6,6\}$. *Since $-1 \in W(E_7)$, the number of elements with trace t is equal to the number elements of trace $-t$. The number of elements of $W(E_7)$ with each trace value is given by the following table:*

Trace	0	1	2	3	4	5	7
$\#W(E_7)$	1128384	722883	151424	12285	672	63	1

.

In Chapter 6 we will state the analogous result for the Weyl group of D_5 when we discuss del Pezzo surfaces of degree 4. Using this Proposition together with the Proposition 24 proves the statement that opened this chapter, Proposition 4.

Note that these counts for elements of the Weyl group of E_7 with given trace match the q^6 coefficients in the polynomials in the statement of Theorem 3, including the $T = 6$ case where this coefficient is 0. In the next section we will see that Elkies' result for point counts of cubic surfaces gives the analogous result for traces of elements of $W(E_6)$. For each surface S we consider the permutation of (-1)-curves given by Frobenius and ask for its conjugacy class in the relevant Weyl group G. Consider the set of all weak del Pezzo surfaces of degree d over $\mathbb{F}_q$ together with a geometric basis. This can be given the structure of a moduli space. They relevant Weyl group acts on this variety. The quotient gives the surface without the basis. An application of the Čebotarev density theorem for extensions of function fields of varieties shows that if we consider all anti-canonical models of del Pezzo surfaces of degree d over $\mathbb{F}_q$ as q goes to infinity, the proportion for which this permutation is in a conjugacy class $C \subseteq G$ is equal to $|C|/|G|$. See Theorem 1 of [**29**] for the type of Čebotarev density statement needed here. We omit the details.

In the rest of this chapter we will consider two situations. First, we give a detailed sketch of the theorem of Elkies giving the weight enumerator of a 20-dimensional code coming from homogeneous cubics on $\mathbb{P}^3(\mathbb{F}_q)$. We then discuss the analogue for del Pezzo surfaces of degree 2 and set up the calculations that will be done in Chapters 3 and 4. The difficulty in each of these theorems is computing the polynomials that count the number of codewords corresponding to a del Pezzo surface of trace t, or equivalently, whose anti-canonical model has $q^2+q+1+tq$ $\mathbb{F}_q$-rational points. Let k be the degree of the sum of these polynomials. The asymptotic result of the previous paragraph is enough to determine the q^k coefficient of each of these polynomials. The hard work comes in finding the entire polynomial explicitly.

4. Point Counts for Cubic Surfaces

In this section we will give a detailed outline of the proof of the following result of Elkies [**20**].

Theorem 26. *The following table lists for each $T \in [-3,6]$, the number of irreducible cubics of cone dimension zero giving a codeword of weight $q^3 - Tq$. For $T \neq 0$ this also counts the number of cubics giving a codeword of weight $q^3 + Tq$. The number is*

given as a multiple of $|\mathrm{GL}_4(\mathbb{F}_q)|/51840$.

T	$51840/\lvert\mathrm{GL}_4(\mathbb{F}_q)\rvert$ *times the number of* $f_3(w,x,y,z)$ *of weight* q^3-Tq
-3	$80(q+1)^2(q^2+q+3)$
-2	$\frac{45}{q+1}(77q^5+34q^4+90q^3+152q^2+281q-26)$
-1	$\frac{72}{q^3-q}(162q^7+325q^6-249q^5+205q^4+177q^3+670q^2+30q-360)$
0	$\frac{12}{q^2(q^2-1)(q^3-1)}\Big(1735q^{11}+1329q^{10}+3314q^9-225q^8+6846q^7$ $-3993q^6+2546q^5+4785q^4+4999q^3+264q^2-12960q-4320\Big)$
1	$\frac{72}{\lvert GL_2(\mathbb{F}_q)\rvert}\Big(182q^8-57q^7+90q^6+840q^5-1262q^4+1907q^3$ $+1350q^2-2690q+360\Big)$
2	$\frac{90}{q-1}(27q^5+20q^4+136q^3-374q^2+1229q-990)$
3	$120(2q^4+9q^3-27q^2+182q-270)$
4	$36(q^4-5q^3+59q^2-235q+260)$
5	$72(q-4)(q-3)(q-2)$
6	$(q-5)^2(q-3)(q-2)$

We follow the same strategy described in Chapter 1. A homogeneous cubic $f_3(w,x,y,z)$ is determined by 20 coefficients, so we get a 20-dimensional code $C_{3,3}$ over $\mathbb{F}_q^{q^3+q^2+q+1}$. The goal is to compute $W_{C_{3,3}}(X,Y)$, and the previous theorem is the most difficult part of this computation.

Most of these q^{20} polynomials cut out a variety $f_3(w,x,y,z)=0$ that is a possibly singular cubic surface, the anti-canonical model of a weak del Pezzo surface of degree 3. The only $f_3(w,x,y,z)$ that do not give such a surface are those that have non-isolated singularities and those that are cones over smooth plane cubics in $\mathbb{P}^2(\mathbb{F}_q)$.

It is elementary to count the cubics that give a variety with non-isolated singularities. There are only a few types of varieties that occur, for example, a triple plane, or a smooth quadric together with a plane. One can write down the contribution to

the weight enumerator coming from such cubics without too much difficulty. See [**20**] for details.

One must also understand the contribution to the weight enumerator from cones over smooth plane cubics. Let p be the vertex of this cone and choose any plane in $\mathbb{P}^3(\mathbb{F}_q)$ not containing p. The cone can be understood as the union of the lines between p and some cubic curve in this plane. If the plane cubic has t $\mathbb{F}_q$-points, then the resulting cone has $1 + qt$ points. Therefore, in order to understand the contribution to $W_{C_{3,3}}(X, Y)$ from cones, we need to understand the weight enumerator of cubics in $\mathbb{P}^2(\mathbb{F}_q)$, $W_{C_{2,3}}(X, Y)$.

A smooth plane cubic is a genus 1 curve. Hasse's theorem, which is stated in the next chapter, shows that every genus 1 curve over $\mathbb{F}_q$ has an $\mathbb{F}_q$-point, and is therefore an elliptic curve. In the next chapter we will discuss some of the theory of elliptic curves over finite fields and how it is used to compute the weight enumerator for plane cubics. We note that the contribution to the weight enumerator from cones over singular plane cubics can be determined by elementary methods, and that such a cone has non-isolated singularities.

Every homogeneous cubic $f_3(w, x, y, z)$ that gives a variety with no isolated singularities and is not a cone cuts out a cubic surface in $\mathbb{P}^3(\mathbb{F}_q)$. Some of these surfaces are singular, but each is the anti-canonical model of some weak del Pezzo surface of degree 3. We consider the minimal desingularization of this surface and choose a geometric basis for its Picard group. This gives $\mathrm{Tr}(\varphi|_{E_6})$. We can determine the sublattice $\mathcal{R}$ generated by (-2)-curves by first studying the singularities of the cubic surface. Once we have found (-2)-curves generating $\mathcal{R}$ written in terms of the geometric basis, we find $\mathrm{Tr}(\varphi|_{\mathcal{R}})$. Theorem 23 together with these facts about singular cubic surfaces shows that such a surface must have $q^2 + q + 1 + tq$ $\mathbb{F}_q$-rational points for some $t \in [-3, 6]$.

Once we have analyzed cubics with non-isolated singularities and cones over plane cubics, $W_{C_{3,3}}(X,Y)$ is determined except for 10 unknown terms:

$$W^{\mathrm{DP}}_{C_{3,3}}(X,Y) := a_{-3}X^{q^2-2q+1}Y^{q^3+3q} + a_{-2}X^{q^2-q+1}Y^{q^3+2q} + \cdots + a_6X^{q^2+7q+1}Y^{q^3-6q}.$$

Determining these unknown coefficients is equivalent to understanding how the values of the trace of Frobenius are distributed as we consider all weak del Pezzo surfaces that are given by homogeneous cubics. We know the sum of these coefficients; it is q^{20} minus the number of cubics that give one of the more singular varieties, a number we have already computed. It is not known how to compute this distribution of trace values directly, so one of the key ideas of Elkies is to use information about $C^{\perp}_{3,3}$ to solve for these unknowns [**20**].

By the MacWilliams theorem, the weight enumerator of $C^{\perp}_{3,3}$ is determined by the weight enumerator of $C_{3,3}$. We see that

$$W_{C_{3,3}}(X,Y) = W^{\mathrm{DP}}_{C_{3,3}}(X,Y) + W^{s}_{C_{3,3}}(X,Y) + W^{G1}_{C_{3,3}}(X,Y),$$

where $W^{s}_{C_{3,3}}(X,Y)$ is the contribution to the weight enumerator from cubics that have non-isolated singularities and $W^{G1}_{C_{3,3}}(X,Y)$ is the contribution to the weight enumerator from cones over smooth plane cubics. The notation reflects the fact that a smooth plane cubic is a genus 1 curve. Therefore,

$$\begin{aligned} W_{C^{\perp}_{3,3}}(X,Y) &= \frac{1}{q^{20}}\Bigg(W^{\mathrm{DP}}_{C_{3,3}}(X+(q-1)Y, X-Y) + \\ &\qquad W^{s}_{C_{3,3}}(X+(q-1)Y, X-Y) + W^{G1}_{C_{3,3}}(X+(q-1)Y, X-Y)\Bigg). \end{aligned}$$

We consider only the dual coefficients up to weight 9, that is, $W_{C^{\perp}_{3,3}}(X,Y)$ modulo Y^{10}.

The contribution from the singular cubics $W^{s}_{C_{3,3}}(X+(q-1)Y, X-Y)$ modulo Y^{10} is $\sum_{i=0}^{9} s_i(q)X^{q^3+q^2+q+1-i}Y^i$, where each $s_i(q)$ is a polynomial. In fact, we could

expand this series as far out as we want, and all of its coefficients will be given by polynomials in q.

The cones over smooth plane cubics are more complicated. As we will explain in the next chapter in some detail, computing the Y^t coefficient of the dual of the code of cubics on $\mathbb{P}^2(\mathbb{F}_q)$ is related to computing the sum of the trace of Frobenius acting on E raised to the power t as E varies through all isomorphism classes of elliptic curves over $\mathbb{F}_q$. Once $t \geq 10$, these powers of traces involve the Fourier series expansions of modular forms. However, for this computation we avoid these issues. It is still true that $W^{G1}_{C_{3,3}}(X+(q-1)Y, X-Y)$ modulo Y^{10} is also $\sum_{i=0}^{9} r_i(q) X^{q^3+q^2+q+1-i} Y^i$, where each $r_i(q)$ is a polynomial in q.

By expanding powers of $(X + (q-1)Y)^{q^3+q^2+q+1-i}(X-Y)^i$, it is clear that $W^{\mathrm{DP}}_{C_{3,3}}(X + (q-1)Y, X - Y)$ modulo Y^{10} equals

$$\sum_{i=0}^{9} u_i(a_{-3}, \ldots, a_6, q) X^{q^3+q^2+q+1-i} Y^i,$$

where for each i, $u_i(a_{-3}, \ldots, a_6, q)$ is linear in each of the a_j and the coefficient of each a_j is a polynomial in q. We therefore see that the number of dual codewords of weight i can be expressed as a linear equation involving polynomials in q and these 10 unknown values of a_j.

We can determine the low-weight coefficients of $C^{\perp}_{3,3}$ directly. The minimal weight dual codewords have weight 6. This is because any five points in $\mathbb{P}^3(\mathbb{F}_q)$ impose independent conditions on cubic polynomials but six points on a line fail to impose independent conditions on cubics. The dual codewords up to weight 9 are not so difficult to count because the support of such a codeword of weight less than 10 must be contained in some two-dimensional linear subspace of $\mathbb{P}^3(\mathbb{F}_q)$, a plane. Therefore, we can find the dual coefficients of weight up to 9 by understanding the low-weight codewords of the simpler code $C^{\perp}_{2,3}$, the dual of the code of cubics in $\mathbb{P}^2(\mathbb{F}_q)$.

Once we have found the number of dual codewords of weight i for $i \in [1, 9]$ we have 9 linear equations in 9 unknowns a_j. There are 10 a_j that we are trying to find, but since we know their sum we have only 9 unknowns. Alternatively, since we know the $X^{q^3+q^2+q+1}$ coefficient of $C_{3,3}^{\perp}$ is 1, we can think of this as 10 linear equations in 10 unknowns. Using standard techniques of linear algebra over $\mathbb{Q}[q]$, we compute the values a_j as polynomials in q, proving Theorem 26. In the next section we will describe how this approach becomes more complicated for the code of double covers of $\mathbb{P}^2$ branched over a plane quartic.

5. Codes from Degree 2 del Pezzo Surfaces

We now turn to the main topic of this thesis, the determination of rational point count distributions for del Pezzo surfaces of degree 2. We study the weight enumerator of a particular 16-dimensional code. We have already seen in Theorem 10 that studying anti-canonical models of del Pezzo surfaces of degree 2 is equivalent to studying double covers of $\mathbb{P}^2$ branched over a plane quartic with at most simple singularities.

A homogeneous quartic in $f_4(x, y, z)$ on $\mathbb{P}^2(\mathbb{F}_q)$ is determined by 15 coefficients. We consider varieties of the form $\alpha w^2 = f_4(x, y, z)$ where $\alpha \in \mathbb{F}_q$. Such an equation is determined by 16 coefficients. When $\alpha = 0$ such an equation defines a cone over a plane quartic. An equation of the form $\alpha w^2 = f_4(x, y, z)$ defines a homogeneous quartic not on $\mathbb{P}^3(\mathbb{F}_q)$, but on the weighted projective space $\mathbb{P}(2, 1, 1, 1)$ over $\mathbb{F}_q$, where w has weight 2 and the other variables have weight 1. We note that any weighted projective space is an irreducible projective variety, and that $\mathbb{P}(2, 1, 1, 1)$ has a unique singular point, the point where $x = y = z = 0$. For more on the geometry of weighted projective space see [**16**].

We consider the 16-dimensional code coming from evaluation of these homogeneous quartics on $\mathbb{P}(2, 1, 1, 1)$. For $q = 2$ the dimension is actually smaller than 16,

but we have excluded this case by supposing that the characteristic of $\mathbb{F}_q$ is not equal to 2. For characteristic not equal to 2 every homogeneous quartic on $\mathbb{P}(2,1,1,1)$

$$w^2 + wf_2(x,y,z) + f_4(x,y,z) = 0,$$

is equivalent to one of the form $w^2 + f_4(x,y,z) = 0$, by completing the square. This is why we focus only of the quartics of the form $w^2 = f_4(x,y,z)$.

Evaluation gives a map to $\mathbb{F}_q^{q^3+q^2+q+1}$, but we will instead consider the map to $\mathbb{F}_q^{q^3+q^2+q}$ where we omit the singular point, $x = y = z = 0$. Let $C'_{2,4} \subset \mathbb{F}_q^{q^3+q^2+q}$ be the 16-dimensional linear code given by the image of this map. We choose this notation because $C_{2,4}$ denotes the code of homogeneous quartics on $\mathbb{P}^2(\mathbb{F}_q)$, and this related code consists of double covers of $\mathbb{P}^2$ branched over these quartics as varieties in weighted projective space. Our goal is to study the contribution to $W_{C'_{2,4}}(X,Y)$ from varieties of the form $w^2 = f_4(x,y,z)$. Equivalently, we determine the weight enumerator of the nonlinear code of size q^{15} coming from quartics on $\mathbb{P}(2,1,1,1)$ of the form $w^2 = f_4(x,y,z)$. This weight enumerator is called $W^D_{C'_{2,4}}(X,Y)$ below. This is also equivalent to determining the specialization $\mathrm{QR}_{C_{2,4}}(X, X^2, 1)$ of the quadratic residue weight enumerator of the 15-dimensional code of plane quartics.

The most difficult part of this problem is the content of Theorem 3. We have already seen that any variety of the form $w^2 = f_4(x,y,z)$ where $f_4(x,y,z)$ has at most simple singularities comes from the anti-canonical map of a possibly singular del Pezzo surface of degree 2 and that such a variety has $q^2 + q + 1 + tq$ $\mathbb{F}_q$-points, for some t satisfying $|t| \leq 7$.

We now break up $W_{C'_{2,4}}(X,Y)$ into $W_{C^c_{2,4}}(X,Y) + (q-1)W^D_{C'_{2,4}}(X,Y)$, where $C^c_{2,4}$ is the code of cones over plane quartics, the 15-dimensional subcode of $C'_{2,4}$ given by $\alpha = 0$, and $W^D_{C'_{2,4}}(X,Y)$ is the contribution to the weight enumerator from equations of the form $w^2 = f_4(x,y,z)$ as $f_4(x,y,z)$ varies through all q^{15} homogeneous quartics. We note that the codewords coming from equations of this type do not constitute a

linear code, which is why we allow α to vary, but for any nonzero α the contribution to the weight enumerator of $C'_{2,4}$ is the same.

Our goal is to compute $W^D_{C'_{2,4}}(X,Y)$. We do this by breaking it up into three parts. We let $W^s_{C'_{2,4}}(X,Y)$ be the contribution to this weight enumerator from equations of the form $w^2 = f_4(x,y,z)$ where $f_4(x,y,z) = 0$ defines a plane quartic with non-isolated singularities, or equivalently, a quartic with a double component. We let $W^{G1}_{C'_{2,4}}(X,Y)$ be the contribution to this weight enumerator from equations of the form $w^2 = f_4(x,y,z)$ where $f_4(x,y,z) = 0$ is the union of four distinct coincident lines. Such a union of lines has a non-simple elliptic singularity. We chose this terminology to reflect the fact that such a variety is a cone over a curve of genus 1 given as a double cover of $\mathbb{P}^1$. We explain this below. We define $W^{DP}_{C'_{2,4}}(X,Y)$ to be the contribution to the weight enumerator from everything else, that is, anti-canonical models of del Pezzo surfaces of degree 2.

We have

$$W^D_{C'_{2,4}}(X,Y) = W^s_{C'_{2,4}}(X,Y) + W^{G1}_{C'_{2,4}}(X,Y) + W^{DP}_{C'_{2,4}}(X,Y).$$

By Proposition 4 we can write

$$W^{DP}_{C'_{2,4}}(X,Y) = a_{-7}X^{q^2+q+1-(-7q)}Y^{q^3-7q-1} + \cdots + a_7 X^{q^2+q+1-(7q)}Y^{q^3+7q-1}.$$

Our goal is to solve for these 15 unknown coefficients. Since $-1 \in W(E_7)$, or equivalently because we can multiply any quartic $f_4(x,y,z)$ by a non-square, we have $a_j = a_{-j}$. So, we are really solving for 8 unknown coefficients. The values of these 8 unknowns are the content of Theorem 3. We note that since -1 is not an element of $W(E_6)$ we do not get a similar relation between point counts for cubic surfaces of trace t and $-t$. In fact, the set of t that occur when studying cubic surfaces is not symmetric with respect to multiplication by -1.

At the end of Chapter 3, we determine $W^s_{C'_{2,4}}(X,Y)$ by elementary, but rather intricate, counting. There is a small set of types of quartics that contribute to this weight enumerator. For example, $f_4(x,y,z)$ can be $\beta(f_2(x,y,z))^2$ where $\beta \in \mathbb{F}_q^*$ and $f_2(x,y,z) = 0$ defines a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$. We can count the number of such quartics and the number of points on the corresponding varieties with little trouble.

In Chapter 3, we determine $W^{G1}_{C'_{2,4}}(X,Y)$ by studying elliptic curves over finite fields. Suppose $f_4(x,y,z)$ gives the union of four distinct coincident lines. For such a quartic to be defined over $\mathbb{F}_q$ it is clear that this common point must be an $\mathbb{F}_q$-rational point. By applying an automorphism of $\mathbb{P}^2(\mathbb{F}_q)$ we can suppose that this point is $[0:0:1]$. We write

$$f_4(x,y,z) = b_0 z^4 + b_1 z^3 + b_2 z^2 + b_3 z + b_4,$$

where each b_i is a homogeneous polynomial of degree i in x and y. Since $f_4(x,y,z)$ has a zero of degree 4 at the point $[0:0:1]$, we see that $b_0 = b_1 = b_2 = b_3 = 0$. Therefore, $f_4(x,y,z)$ is a homogeneous quartic in x and y. Such a plane quartic defines a cone over a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$. In case this quartic does not have a double zero, that is, when this quartic on $\mathbb{P}^1(\mathbb{F}_q)$ is smooth, this is a cone over a genus 1 curve. So, in order to determine $W^{G1}_{C'_{2,4}}(X,Y)$ we need only determine the point count distribution for equations of the form $w^2 = f_4(x,y)$ where $f_4(x,y)$ is a smooth homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$. We do this in Chapter 3. In fact, using the quadratic residue weight enumerator defined in the Introduction, we give something stronger, a distribution of point counts that distinguishes between $\mathbb{F}_q$-rational points that come from zeros of $f_4(x,y)$ and points that come from values of $f_4(x,y)$ that are nonzero squares in $\mathbb{F}_q^*$.

At this point, we will have determined all of $W^D_{C'_{2,4}}(X,Y)$ except for the 8 unknowns of $W^{DP}_{C'_{2,4}}(X,Y)$. We will find these by studying dual coefficients of low weight. In the case of cubic surfaces we had 10 unknowns but we also know their sum. We

saw that computing the dual coefficients up to weight 9 gave 10 linear equations involving these unknown coefficients, exactly enough information to solve for them uniquely.

We will compute the contribution to dual codewords of weight up to 7 coming from $W^{DP}_{C'_{2,4}}(X,Y)$. That is, we compute $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^8 by investigating the geometry of points that fail to impose independent conditions on varieties of the form $\alpha w^2 = f_4(x,y,z)$. Unfortunately, this is not enough information to determine these counts uniquely.

In the case of cubic surfaces, we can express the contribution to the dual code coming from the 10 unknown terms as a 10×10 matrix A, where each column corresponds to the contribution to the dual coefficients of weight i, or the Y^i term of this expansion for some $i \in [0,9]$, and each row corresponds to one of the unknowns a_j, for $j \in [-3,6]$. The entries are given by polynomials in q. We then solve a system of linear equations $A\vec{x} = \vec{y}$, where $\vec{x}$ is a column vector with 10 entries corresponding to our unknowns a_j, and $\vec{y}$ is a column vector with entries that are polynomials in q corresponding to the contributions to the dual coefficients of weight up to 9 coming from these ten unknown terms. This equation has a unique solution because this matrix has rank 10.

In the case of del Pezzo surfaces of degree 2, we form an 8×8 matrix where each column corresponds to the contribution to the dual coefficient of weight i, and each row corresponding to the terms of trace $\pm j$. However, this matrix does not have full rank; in fact, the rank is only 4. In order to solve for these eight unknowns we must work harder.

We will determine the contribution to of $W^{DP}_{C'_{2,4}}(X,Y)$ to the dual code coefficients of weight up to 10, that is, $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11}. In order to do this we compute $W_{C'_{2,4}{}^{\perp}}(X,Y)$ modulo Y^{11} by determining the possible supports of dual codewords of weight up to 10, and counting the number of dual

codewords with given support. We do the same for the dual of the 15-dimensional subcode coming from cones over plane quartics, computing $W_{C_{2,4}^c{}^\perp}(X,Y)$ modulo Y^{11}. We compute $W^s_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11} with little trouble. Finding $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11} involves some new difficulties because the weight 10 coefficient is not a polynomial in q, but involves a term of the Fourier series expansion of the modular form Δ.

In the calculation for cubic surfaces, the contribution to the dual codes coefficients from cones over plane cubics was not difficult to determine because the coefficients of $W_{C_{2,3}^\perp}(X,Y)$ up to weight 9 are given by polynomials in q. The weight 10 coefficient involves the Ramanujan tau function, $\tau(q)$, which is the qth coefficient of the Fourier series expansion of the modular form Δ. Since this calculation did not require the dual code coefficients of weight larger than 9, this complication was avoided. However, for del Pezzo surfaces of degree 2, we will see that the Y^{10} term of $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ also involves $\tau(q)$, as does the Y^{10} term of $W_{C'_{2,4}{}^\perp}(X+(q-1)Y, X-Y)$ because it includes this contribution from cones over genus 1 curves. In this setting we really do need to analyze these non-elementary terms. We will explain this issue in Chapter 3.

We see that

$$(q-1)W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y) = q^{16}W_{C'_{2,4}{}^\perp}(X,Y) - q^{15}W_{C_{2,4}^c{}^\perp}(X,Y) -$$
$$(q-1)\left(W^s_{C'_{2,4}}(X+(q-1)Y, X-Y) + W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)\right).$$

We compute the right-hand side of this equation modulo Y^{11}. This lets us compute $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y) \pmod{Y^{11}}$. Individual terms of the right-hand side involve $\tau(q)$, but these non-elementary terms cancel out. We will express this as an 8×10 matrix with entries that are polynomials in q. This matrix has rank 6. So, we still do not have enough information to solve for the eight unknowns a_j, for $j\in[0,7]$.

We use the geometry of blow-ups of $\mathbb{P}^2$ at seven points to find a_7 and a_6 directly. This involves counting 7-tuples of points in $\mathbb{P}^2(\mathbb{F}_q)$ in general position to find a_7, and in what we call near general position to find a_6. A key observation is that we can understand surfaces of trace 7 and 6 by considering blow-ups of $\mathbb{P}^2$ at seven points of $\mathbb{P}^2(\mathbb{F}_q)$ that are actually $\mathbb{F}_q$-rational points.

Given a fixed 4-tuple of points (p_1, p_2, p_3, p_4) in $\mathbb{P}^2(\mathbb{F}_q)$, no three of them on a line, let $S(q)$ denote the number of choices of an ordered set of points in $\mathbb{P}^2(\mathbb{F}_q)$, (p_5, p_6, p_7), such that the points $p_1, \ldots, p_7$ are in general position. Since $\mathrm{PGL}_3(\mathbb{F}_q)$ acts simply transitively on collections of four points, no three of which lie on a line, the number of 7-tuples of points of $\mathbb{P}^2(\mathbb{F}_q)$ in general position is $|\mathrm{PGL}_3(\mathbb{F}_q)|S(q)$.

Similarly, let $R(q)$ denote the number of choices of an ordered tuple of points in $\mathbb{P}^2(\mathbb{F}_q)$, (p_5, p_6, p_7), such that the points $p_1, \ldots, p_7$ satisfy the following conditions

(1) no three points lie on a line,

(2) there is a unique smooth conic that contains exactly 6 of the 7 points.

We say that a 7-tuple of points satisfying these hypotheses is in *near general position*. The number of 7-tuples of points of $\mathbb{P}^2(\mathbb{F}_q)$ in near general position is $|\mathrm{PGL}_3(\mathbb{F}_q)|R(q)$.

Theorem 27. *Let $W^{DP}_{C'_{2,4}}(X, Y)$ be defined as above. Then*

$$a_7 = \frac{|\mathrm{GL}_3(\mathbb{F}_q)|S(q)}{|W(E_7)|},$$

and

$$a_6 = \frac{18|\mathrm{GL}_3(\mathbb{F}_q)|R(q)}{|W(E_7)|}.$$

In Chapter 4 we will prove this result and use the geometry of $\mathbb{P}^2(\mathbb{F}_q)$ to determine $S(q)$ and $R(q)$. This requires us to investigate the Picard group of a surface with a single (-2)-curve in detail.

We can now write down a modified version of the matrix described above, which is now 6×10 and has rank 6. The resulting matrix equation has a unique solution, giving Theorem 3.

There is an interesting issue related to this computation. We determine the low-weight dual code coefficients of the 15-dimensional code of cones over plane quartics. This is equivalent to finding $W_{C_{2,4}^c}(X + (q-1)Y, X - Y)$ modulo Y^{11}. With our current techniques it is hopeless to try to find $W_{C_{2,4}^c}(X, Y)$ completely, because this is equivalent to finding $W_{C_{2,4}}(X, Y)$, the weight enumerator of the code of homogeneous quartics in $\mathbb{P}^2(\mathbb{F}_q)$. A generic homogeneous quartic defines a smooth genus 3 curve. There are many difficulties with questions about rational points on genus 3 curves over finite fields that do not arise for the far easier case of plane cubics, or for more general genus 1 curves over finite fields. Even though we cannot hope to determine $W_{C_{2,4}}(X, Y)$, we are able to compute the specialization of the residue weight enumerator $\mathrm{QR}_{C_{2,4}}(X, X^2, 1)$. Perhaps this related weight enumerator can say something new for this more difficult situation.

CHAPTER 3

Quadratic Residue Weight Enumerators and Elliptic Curves over Finite Fields

In this chapter we define a weight enumerator that keeps track of more information than the classical Hamming weight enumerator, prove a variation of the MacWilliams theorem for it, and then apply this result to study quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ and elliptic curves over finite fields. The results for elliptic curves will be a applied to study the weight enumerator $W^{G1}_{C'_{2,4}}(X,Y)$ defined in the previous chapter. At the end of this chapter we also compute $W^{s}_{C'_{2,4}}(X,Y)$ by studying double covers of $\mathbb{P}^2$ branched over plane quartics with non-isolated singularities.

1. The MacWilliams Theorem

We begin by giving a proof of the MacWilliams theorem using discrete Poisson summation. We then adapt this proof to give a version of this result that applies to the quadratic residue weight enumerator.

Lemma 28 (Discrete Poisson summation)**.** *Let G be a finite abelian group, $H \subset G$ a subgroup, $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ the character group of G, and $H^* = \{\hat{g} \in \widehat{G} \mid \forall h \in H,\ \widehat{g}(h) = 1\}$ the annihilator of H in $\widehat{G}$. For any function ϕ on G define the Fourier transform of ϕ to be the function on $\widehat{G}$ given by*

$$\hat{\phi}(\hat{g}) = \sum_{g \in G} \hat{g}(g)\phi(g).$$

Then

$$[G : H] \sum_{h \in H} \phi(h) = \sum_{h^* \in H^*} \hat{\phi}(h^*).$$

See Chapter 12 of [**48**] for a proof. The main idea is to choose a function that gives some information about an element of $\mathbb{F}_q^N$, for example, its number of nonzero coordinates. We sum this function over the elements of a linear code. Taking the sum of the Fourier transform of this function over the dual code gives an identity. Since the Fourier transform is given in terms of certain sums of characters, this strategy only works in cases where we can compute the relevant character sums. We recall a simple lemma.

Lemma 29. *Let ψ be a non-trivial character on $\mathbb{F}_q$. Suppose $g = (g_1, \ldots, g_N) \in \mathbb{F}_q^N \setminus (0, \ldots, 0)$. Then*

$$\sum_{h \in \mathbb{F}_q^N \setminus (0,\ldots,0)} \psi(\langle g, h \rangle) = -1.$$

PROOF. The map $h \to \psi(\langle g, h \rangle)$ is a character on the finite additive group $\mathbb{F}_q^N$. Therefore, the sum of this character over all h vanishes unless it is the trivial character, which is the case if and only if $g = (0, \ldots, 0)$. We see that

$$\sum_{h=(h_1,\ldots,h_N) \in \mathbb{F}_q^N \setminus (0,\ldots,0)} \prod_{i=1}^{N} \psi(g_i h_i) = 0 - \prod_{i=1}^{N} \psi(0) = -1.$$

□

We recall the statement of the MacWilliams theorem for the Hamming weight enumerator. This is Theorem 1 in the Introduction, but we state it again here.

Theorem 30 (MacWilliams)**.** *Let C be a linear code over $\mathbb{F}_q^N$ and $C^\perp$ be its dual code. Then*

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y).$$

PROOF. Let ψ be a non-trivial character on $\mathbb{F}_q$. We let $G = \mathbb{F}_q^N$ and identify $\hat{G}$ with G by identifying the element $g \in \mathbb{F}_q^N$ with the character taking $h \in \mathbb{F}_q^N$ to $\psi(\langle g, h \rangle)$. A linear code C is a subgroup of G and $\hat{C}$ is identified with $C^\perp$. The index $[G : C]$ is equal to $q^n/|C| = |C^\perp|$.

Let $g = (g_1, \ldots, g_N) \in \mathbb{F}_q^N$ and define

$$\phi(g) := \prod_{i=1}^{N} F(g_i), \text{ where } F(g_i) := \begin{cases} X & \text{if } g_i = 0, \\ Y & \text{otherwise} \end{cases}.$$

Then

$$\hat{\phi}(\hat{g}) = \sum_{g \in \mathbb{F}_q^N} \psi(\langle g, \hat{g} \rangle) \phi(g).$$

We take the sum of ϕ over all elements of C and get

$$\sum_{c \in C} \phi(c) = W_C(X, Y).$$

Discrete Poisson summation implies that

$$W_C(X, Y) = \frac{1}{|C^\perp|} \sum_{d \in C^\perp} \hat{\phi}(d).$$

We consider the coordinates of $d = (d_1, \ldots, d_N)$ one at a time. Note that

$$\hat{\phi}(d) = \sum_{g \in \mathbb{F}_q^N} \psi(\langle d, g \rangle) \phi(g) = \prod_{i=1}^{N} \sum_{g_i \in \mathbb{F}_q} \psi(d_i g_i) F(g_i),$$

where $g = (g_1, \ldots, g_N)$. For some fixed value of i,

$$\sum_{g_i \in \mathbb{F}_q} \psi(d_i g_i) F(g_i) = \begin{cases} X + (q-1)Y & \text{if } d_i = 0 \\ X - Y & \text{otherwise,} \end{cases}$$

since

$$\sum_{g_i \in \mathbb{F}_q^*} \psi(d_i g_i) F(g_i) = Y \sum_{g_i \in \mathbb{F}_q^*} \psi(d_i g_i) = -Y,$$

by the previous lemma.

We take the product over all coordinates $i \in [1, N]$ and have

$$W_C(X,Y) = \frac{1}{|C^\perp|} \sum_{d \in C^\perp} \prod_{i=1}^{N} F'(d_i), \text{ where } F'(d_i) = \begin{cases} X + (q-1)Y & \text{if } d_i = 0 \\ X - Y & \text{otherwise} \end{cases}.$$

This last sum is $\frac{1}{|C^\perp|} W_{C^\perp}(X + (q-1)Y, X - Y)$, completing the proof.

□

2. MacWilliams Theorem for the Quadratic Residue Weight Enumerator

In the previous argument we encountered some elementary character sums. We need only the most basic facts about characters to evaluate them. In proving analogues of the MacWilliams theorem for more refined weight enumerators we need to understand more complicated character sums. We next turn to one of the simplest non-trivial examples, quadratic Gauss sums.

Proposition 31. *Suppose that $q = p^k$ is odd where p is prime and $k \geq 1$. Let ψ be an additive character on $\mathbb{F}_q$. Then*

$$\sum_{x \in \mathbb{F}_q^*} \psi(x^2) = \epsilon_q \sqrt{q}, \text{ where } \epsilon_q = \begin{cases} 1 \text{ if } q \equiv 1 \pmod 4 \\ i \text{ if } q \equiv 3 \pmod 4 \end{cases}.$$

Many number theory textbooks contain a proof of this fact, for example, see Chapter 8 of [**27**]. We use this fact to give a proof of the MacWilliams identity for the quadratic residue weight enumerator defined in the Introduction.

We first recall the definition of this weight enumerator. Let C be a linear code defined over $\mathbb{F}_q^N$. Let R denote the set of nonzero squares in $\mathbb{F}_q^*$ and NR denote the set of non-squares. We define the quadratic residue weight enumerator by

$$\mathrm{QR}_C(X,Y,Z) = \sum_{c \in C} X^{N - \mathrm{wt}(c)} Y^{\mathrm{Res}(c)} Z^{\mathrm{NRes}(c)},$$

where $\mathrm{Res}(c)$ is equal to the number of coordinates of c in R and $\mathrm{NRes}(c)$ is the number of coordinates of c in NR. It is clear that $\mathrm{Res}(c) + \mathrm{NRes}(c) = \mathrm{wt}(c)$. We can write this weight enumerator as a product over coordinates

$$\mathrm{QR}_C(X,Y,Z) = \sum_{c=(c_1,\ldots,c_N)\in C} \prod_{i=1}^{N} F(c_i), \text{ where } F(c_i) = \begin{cases} X \text{ if } c_i = 0 \\ Y \text{ if } c_i \in R \\ Z \text{ if } c_i \in NR. \end{cases}.$$

We now state the MacWilliams theorem for this quadratic residue weight enumerator.

Theorem 32. *Let $C \subseteq \mathbb{F}_q^N$ be a linear code. Then $\mathrm{QR}_C(X,Y,Z)$ equals $|C^\perp|^{-1}$ times*

$$\mathrm{QR}_{C^\perp}\left(X + \frac{q-1}{2}(Y+Z), X - Z + \frac{\epsilon\sqrt{q}-1}{2}(Y-Z), X - Y + \frac{\epsilon\sqrt{q}-1}{2}(Z-Y)\right),$$

where

$$\epsilon = \begin{cases} 1 & \text{if } \mathrm{char}(q) \equiv 1 \pmod 4 \\ \sqrt{-1} & \text{if } \mathrm{char}(q) \equiv 3 \pmod 4 \end{cases}.$$

Proof. Let $\phi(c)$ be defined by $\prod_{i=1}^{N} F(c_i)$ where F is defined above. Then

$$\sum_{c\in C} \phi(c) = \sum_{c\in C} X^{N-wt(c)} Y^{\mathrm{Res}(c)} Z^{\mathrm{NRes}(c)} = \mathrm{QR}_C(X,Y,Z).$$

The Fourier transform of ϕ is defined by

$$\hat{\phi}(\hat{g}) = \sum_{g\in\mathbb{F}_q^N} \psi(\langle g, \hat{g}\rangle)\phi(g).$$

Discrete Poisson summation gives

$$\mathrm{QR}_C(X,Y,Z) = \sum_{c\in C} \phi(c) = \frac{1}{|C^\perp|} \sum_{d\in C^\perp} \hat{\phi}(d).$$

We consider the coordinates of $\hat{\phi}(d)$ one at a time. We have

$$\begin{aligned}\hat{\phi}(d) &= \sum_{g=(g_1,\ldots,g_N)\in\mathbb{F}_q^N} \prod_{i=1}^{N} \psi(d_i g_i) F(g_i) = \prod_{i=1}^{N} \sum_{g_i\in\mathbb{F}_q} \psi(d_i g_i) F(g_i) \\ &= \prod_{i=1}^{N} \left(X + Y \sum_{x\in R} \psi(x d_i) + Z \sum_{x\in NR} \psi(x d_i) \right).\end{aligned}$$

Consider the expression within the product. If $d_i = 0$ this is $X + \frac{q-1}{2}(Y+Z)$. If $d_i \in R$, this is

$$X + Y \sum_{x\in R} \psi(x) + Z \sum_{x\in NR} \psi(x).$$

If $d_i \in NR$, this is

$$X + Y \sum_{x\in NR} \psi(x) + Z \sum_{x\in R} \psi(x).$$

The previous result on quadratic Gauss sums shows that

$$\sum_{x\in R} \psi(x) = \epsilon_q \sqrt{q}, \text{ and } \sum_{x\in NR} \psi(x) = -\left(1 + \epsilon_q \sqrt{q}\right),$$

since $\sum_{x\in\mathbb{F}_q^*} \psi(x) = -1$.

Rearranging terms implies that $\hat{\phi}(d)$ equals

$$\left(X + \tfrac{q-1}{2}(Y+Z)\right)^{N-\mathrm{wt}(d)} \qquad \left(X - Z + \frac{\epsilon\sqrt{q}-1}{2}(Y-Z)\right)^{\mathrm{Res}(d)} \cdot$$
$$\left(X - Y + \tfrac{\epsilon\sqrt{q}-1}{2}(Z-Y)\right)^{\mathrm{NRes}(d)} .$$

Summing over all $d \in C^{\perp}$ completes the proof. □

In the final section of this chapter we will use results about cubic Gauss sums to prove a version of the MacWilliams identity for another variation of the Hamming weight enumerator.

3. The Quadratic Residue Weight Enumerator for Quadrics

In the Introduction we considered the quadratic residue weight enumerator for the three-dimensional code $C_{1,2}$ of quadratic polynomials on $\mathbb{P}^1(\mathbb{F}_q)$. We showed that

$$\begin{aligned}\mathrm{QR}_{C_{1,2}}(X,Y,Z) &= X^{q+1} + \frac{(q+1)q(q-1)}{2} X^2 Y^{\frac{q-1}{2}} Z^{\frac{q-1}{2}} \\ &+ \frac{(q-1)(q+1)}{2} X(Y^q + Z^q) + \frac{(q-1)^2 q}{2} Y^{\frac{q+1}{2}} Z^{\frac{q+1}{2}}.\end{aligned}$$

We noted that the $(q-1)\binom{q+1}{4}$ dual codewords of weight 4, contribute

$$\frac{(q-1)^3 q(q+1)}{32} Y^2 Z^2 + \frac{(q-5)(q-1)^2 q(q+1)}{192} \left(Y^4 + Z^4\right),$$

to the quadratic residue weight enumerator of $C_{1,2}^{\perp}$ in the case $q \equiv 1 \pmod 4$ and contribute

$$\frac{(q-3)(q-1)^2 q(q+1)}{32} Y^2 Z^2 + \frac{(q-1)^2 q(q+1)^2}{192} \left(Y^4 + Z^4\right),$$

when $q \equiv 3 \pmod 4$. This is a simple application of the MacWilliams identity given above. We note that for a codeword $c \in C_{1,2}^{\perp}$ of minimum weight, the product of the coordinates of c is in R. We will see that this is common for codes that come from the evaluation of polynomials.

In Elkies' paper [**20**], elementary facts about quadratic forms over finite fields are used to determine $W_{C_{n,2}}(X,Y)$, the weight enumerator of the code of quadrics on $\mathbb{P}^n(\mathbb{F}_q)$ for any n. Our next goal to to determine the quadratic residue weight enumerators of these codes.

We first recall the different types of quadrics that occur in $\mathbb{P}^3(\mathbb{F}_q)$. There are the singular quadrics given by double planes, the union of two distinct rational planes, the union of two Galois-conjugate planes defined over $\mathbb{F}_{q^2}$, and quadric cones. Unlike in $\mathbb{P}^2(\mathbb{F}_q)$ it is not true that all smooth quadrics are isomorphic. There are two isomorphism classes: plus quadrics, which are isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ and

have $(q+1)^2$ $\mathbb{F}_q$-rational points, and minus quadrics, which have q^2+1 $\mathbb{F}_q$-rational points. The different types of quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ will be explained below, and will clarify this special case.

We first compute $\mathrm{QR}_{C_{2,2}}(X,Y,Z)$ following the strategy used for $C_{1,2}$ in the Introduction. Consider the different orbits given by the automorphism group of $\mathbb{P}^2(\mathbb{F}_q)$ acting on the space of quadrics. We need only consider one quadric from each of these different types: double lines, the product of two distinct rational lines, the product of two Galois-conjugate lines, and smooth conics. We consider a representative equation of this type $f(x,y,z)$ and the resulting quadrics in $\mathbb{P}^3(\mathbb{F}_q)$ given by $w^2 = f(x,y,z)$ and $w^2 = \alpha f(x,y,z)$ with α a non-square in $\mathbb{F}_q^*$.

For a double line we choose $f(x,y,z) = x^2$ and note that $w^2 = x^2$ gives the union of two rational planes, and that $w^2 = \alpha x^2$ gives the union of two Galois-conjugate planes. For the product of two rational lines we choose $f(x,y,z) = xy$ and note that both $w^2 = xy$ and $w^2 = \alpha xy$ are quadric cones. For two Galois-conjugate lines we take $f(x,y,z) = -x^2 + \alpha y^2$ where α is a non-square and note that both $w^2 = f(x,y,z)$ and $w^2 = \alpha f(x,y,z)$ give quadric cones. For a smooth conic we take $f(x,y,z) = -x^2 - y^2 - z^2$ and note that $w^2 = f(x,y,z)$ gives a plus quadric on $\mathbb{P}^3(\mathbb{F}_q)$ and $w^2 = \alpha f(x,y,z)$ gives a minus quadric. Putting all of this together and counting the number of quadrics of different types gives the weight enumerator.

Proposition 33. *Let $C_{2,2}$ be the code of quadrics on $\mathbb{P}^2(\mathbb{F}_q)$. Then*

$$\begin{aligned}
\mathrm{QR}_{C_{2,2}}(X,Y,Z) &= X^{q^2+q+1} + \frac{q^3-1}{2}\left(X^{q+1}Y^{q^2} + X^{q+1}Z^{q^2}\right) \\
&+ \frac{q^3-1}{2}(q^2+q)X^{2q+1}Y^{\frac{q^2-q}{2}}Z^{\frac{q^2-q}{2}} + \frac{q^3-1}{2}(q^2-q)XY^{\frac{q^2+q}{2}}Z^{\frac{q^2+q}{2}} \\
&+ \frac{q^3-1}{2}q^2(q-1)\left(X^{q+1}Y^{\frac{q^2+q}{2}}Z^{\frac{q^2-q}{2}} + X^{q+1}Y^{\frac{q^2-q}{2}}Z^{\frac{q^2+q}{2}}\right).
\end{aligned}$$

By being more systematic and using the weight enumerator of quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ from [**20**], we determine the quadratic residue weight enumerator for quadrics on $\mathbb{P}^n(\mathbb{F}_q)$.

We recall the notation

$$(q)_k := \prod_{i=1}^{k-1}(q^k - q^i), \quad \text{and} \quad \binom{n}{i}_q := \prod_{j=0}^{i-1} \frac{(n)_q}{(i)_q(n-i)_q}.$$

The following proposition from [**20**] gives the weight enumerator $W_{C_{n,2}}(X, Y)$.

Proposition 34.

(1) The weight of each $f \in C_{n,2}$ either equals q^n or is of the form $q^n \pm q^{n-\rho}$ for some nonnegative even integer $\rho \leq (n+1)/2$, where the minus sign must be used if $\rho = 0$. Moreover, $\mathrm{wt}(f) = q^n \pm q^{n-\rho}$ if and only if the bilinear form $(\cdot,\cdot)_f$ associated to f defined by $(x, x')_f := f(x+x') - f(x) - f(x')$, has rank 2ρ and f vanishes on its kernel.

(2) Let ρ be such an integer and $\epsilon \in \{\pm 1\}$, with $\epsilon = +1$ if $\rho = 0$. Then the number of $f \in C_{n,2}$ of weight $q^n - \epsilon q^{n-\rho}$ is

$$q^{\rho^2} \frac{q^\rho + \epsilon}{2} \binom{n+1}{2\rho}_q \frac{(2\rho)_q}{(\rho)_{q^2}}.$$

(3) The weight enumerator of $C_{n,2}$ is

$$X^{\frac{q^n-1}{q-1}} Y^{q^n} \left[q^{\binom{n+2}{2}} + \sum_{\rho=0}^{\lfloor \frac{n+1}{2} \rfloor} q^{\rho^2} \frac{(n+1)_q}{(n+1-2\rho)_q (\rho)_q^2} \cdot \left(\frac{q^\rho + 1}{2} \frac{X}{Y}^{q^{n-\rho}} + \frac{q^\rho - 1}{2} \frac{X}{Y}^{q^{-n-\rho}} - q^\rho \right) \right]$$

The proof of this result relies on some basic facts about quadratic forms over finite fields given in [**20**]. We recall that we have assumed that the characteristic of $\mathbb{F}_q$ is not 2. Let f be a quadratic form on a vector space V and W be the kernel of the bilinear form associated to f. Then f descends to a well-defined nondegenerate

form $\overline{f}$ on the cokernel V/W. Let $r = \dim(V/W)$. The weight of f as an element of $C_{n,2}$ is determined by the weight of $\overline{f}$ as an element of $C_{r-1,2}$. If r is odd then all nondegenerate f are $\mathrm{GL}_r(\mathbb{F}_q)$ equivalent and the associated forms on $C_{n,2}$ all have weight q^n. We note that the stabilizer of such a form on an r dimensional vector space has size $(q^r - q)(q^r - q^3)\cdots(q^r - q^{r-2})$. We count the number of quadratic forms with r odd by first counting the number of r dimensional subspaces of $\mathbb{P}^n(\mathbb{F}_q)$ and then counting the number of quadratic forms of rank r on each one. This gives

$$\frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})}\cdot\frac{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})}{(q^r-q)(q^r-q^3)\cdots(q^r-q^{r-2})}.$$

When r is even things are more complicated. There are two $\mathrm{GL}_r(\mathbb{F}_q)$ inequivalent forms and they are defined by their Witt index. There are

$$q^{\rho^2}\frac{q^\rho+1}{2}\frac{(2\rho)_q}{(\rho)_q^2}$$

forms $f \in C_{2\rho-1,2}$ with Witt index ρ, and each has weight $q^{\rho-1}(q^\rho - 1)$. Similarly, there are

$$q^{\rho^2}\frac{q^\rho-1}{2}\frac{(2\rho)_q}{(\rho)_q^2}$$

forms $f \in C_{2\rho-1,2}$ with Witt index $\rho-1$, and each has weight $q^{\rho-1}(q^\rho+1)$. Combining these observations gives the proposition.

We now want to give the quadratic residue weight enumerator for $C_{n,2}$. For each form in $C_{n,2}$ with rank $\dim(V/W)$ described above, we know the number of rational points. We want to determine how many of the $\mathrm{wt}(f)$ nonzero coordinates of f are nonzero squares and how many are non-squares. This is equivalent to knowing the number of rational points on the quadric $w^2 = f(x_0, \ldots, x_n)$. This is a quadric in $\mathbb{P}^{n+1}(\mathbb{F}_q)$ with rank one larger than the rank of f. Therefore, if f has even rank then this form has odd rank, and if f has odd rank then this form has even rank.

All forms of rank $r+1$ where $r+1$ is odd are $\mathrm{GL}_{r+1}(\mathbb{F}_q)$ equivalent and give rise to quadrics with the same weight, q^{n+1}, as elements of $C_{n+1,2}$. All f of odd rank r are $\mathrm{GL}_r(\mathbb{F}_q)$ equivalent to a single form of rank r, f_r, and whether the associated form of rank $r+1$ has Witt index $\frac{r+1}{2}$ or $\frac{r+1}{2}-1$ depends solely on whether f if $\mathrm{PGL}_r(\mathbb{F}_q)$ equivalent to f_r times a nonzero square or times a non-square. Since there are $\frac{q-1}{2}$ non-zero squares and $\frac{q-1}{2}$ non-squares the f of rank r for r odd give rise to the same number of quadrics of rank $r+1$ with each Witt index. This gives the distribution of the number of points on the quadrics of rank $r+1$ coming from forms of rank r.

Proposition 35. *The quadratic residue weight enumerator* $\mathrm{QR}_{C_{n,2}}(X,Y,Z)$ *equals*

$$\begin{aligned}
& X^{\frac{q^n-1}{q-1}}\left[\sum_{\rho=0}^{\lfloor\frac{n+1}{2}\rfloor} q^{\rho^2}\frac{(n+1)_q}{(n+1-2\rho)_q(\rho)_{q^2}}\cdot\right.\\
\cdot\quad & \left.\left(\frac{q^\rho+1}{2}X^{q^{n-\rho}}Y^{\frac{q^n-q^{n-\rho}}{2}}Z^{\frac{q^n-q^{n-\rho}}{2}}+\frac{q^\rho-1}{2}\frac{Y^{\frac{q^n+q^{n-\rho}}{2}}Z^{\frac{q^n+q^{n-\rho}}{2}}}{2X^{q^{n-\rho}}}\right)\right]\\
+\quad & X^{\frac{q^n-1}{q-1}}\left[\sum_{r=0}^{\lfloor\frac{n}{2}\rfloor}\frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^{2r})}{2(q^{2r+1}-q)(q^{2r+1}-q^3)\cdots(q^{2r+1}-q^{2r-1})}\right.\\
& \left.\left(Y^{\frac{q^n+q^{n-r}}{2}}Z^{\frac{q^n-q^{n-r}}{2}}+Y^{\frac{q^n-q^{n-r}}{2}}Z^{\frac{q^n+q^{n-r}}{2}}\right)\right]
\end{aligned}$$

This matches our computations for $\mathrm{QR}_{C_{1,2}}(X,Y,Z)$ and $\mathrm{QR}_{C_{2,2}}(X,Y,Z)$. We first consider $C_{1,2}$. There are two terms in the first sum. The $\rho=0$ term gives X^{q+1} and the $\rho=1$ term gives

$$(q^2-q)\left(\frac{q+1}{2}X^2Y^{\frac{q-1}{2}}X^{\frac{q-1}{2}}+\frac{q-1}{2}Y^{\frac{q+1}{2}}Z^{\frac{q+1}{2}}\right).$$

There is one term, $r=0$, in the second sum. It gives

$$\frac{q^2-1}{2}\left(XY^q+XZ^q\right).$$

Adding these together gives the value of $\mathrm{QR}_{C_{1,2}}(X,Y,Z)$ computed above.

For $\mathrm{QR}_{C_{2,2}}(X,Y,Z)$ the first sum has two terms. For $\rho = 0$ we get X^{q^2+q+1}. For $\rho = 1$ we get

$$q(q^3-1)\left(\frac{q+1}{2}X^{2q+1}Y^{\frac{q^2-q}{2}}Z^{\frac{q^2-q}{2}} + \frac{q-1}{2}XY^{\frac{q^2+q}{2}}Z^{\frac{q^2+q}{2}}\right).$$

The second term also has two terms. The $r = 0$ term gives

$$\frac{q^3-1}{2}\left(X^{q+1}Y^{q^2} + X^{q+1}Z^{q^2}\right).$$

The $r = 1$ term gives

$$\frac{(q^3-1)(q^3-q^2)}{2}\left(X^{q+1}Y^{\frac{q^2+q}{2}}Z^{\frac{q^2-q}{2}} + X^{q+1}Y^{\frac{q^2-q}{2}}Z^{\frac{q^2+q}{2}}\right).$$

Adding these terms together gives the polynomial computed above for $C_{2,2}$.

We now consider the quadratic residue weight enumerator of $C_{n,2}^{\perp}$ using the MacWilliams theorem proven above. The Hamming weight enumerator of the dual of $C_{n,2}$ is given in [**20**]. We do not attempt to compute $\mathrm{QR}_{C_{n,2}^{\perp}}(X,Y,Z)$ in general, but instead focus on small values of n. We begin with $C_{1,2}$. We use the quadratic residue version of the MacWilliams theorem to formally expand the first few terms of the quadratic residue weight enumerator of the dual of $C_{1,2}$. We consider two cases based on the value of ϵ. When $\epsilon = 1$, that is, the characteristic of $\mathbb{F}_q$ is 1 modulo 4, we compute that $\mathrm{QR}_{C^{\perp}}(X,Y)$ is

$$\begin{aligned}
& X^{q+1} + \left(\frac{(q-5)(q-1)^2q(q+1)}{2^6\cdot 3}(Y^4+Z^4) + \frac{(q-1)^3q(q+1)}{2^5}Y^2Z^2\right)X^{q-3} \\
+ \; & \left(\frac{(q-3)(q-1)^2q(q+1)(q^2-6q+53)}{2^8\cdot 3\cdot 5}(Y^5+Z^5)\right. \\
+ \; & \frac{(q-5)(q-3)(q-1)^3q(q+1)}{2^8\cdot 3}(YZ^4+Y^4Z) \\
+ \; & \left.\frac{(q-5)(q-3)(q-1)^3q(q+1)}{2^7\cdot 3}(Y^2Z^3+Y^3Z^2)\right)X^{q-4},
\end{aligned}$$

plus terms involving Y^iZ^j with $i+j \geq 6$.

When $\epsilon = -1$ we compute that $\mathrm{QR}_{C^\perp}(X,Y)$ is

$$\begin{aligned} & X^{q+1} + \left(\frac{(q-1)^2q(q+1)^2}{2^6 \cdot 3}(Y^4+Z^4) + \frac{(q-3)(q-1)^2q(q+1)}{2^5}Y^2Z^2 \right) X^{q-3} \\ + & \left(\frac{(q-7)(q-3)(q-1)^2q(q+1)^2}{2^8 \cdot 3 \cdot 5}(Y^5+Z^5) \right. \\ + & \frac{(q-7)(q-3)(q-1)^2q(q+1)^2}{2^8 \cdot 3}(Y^4Z+YZ^4) \\ + & \left. \frac{(q-3)(q-1)^2q(q+1)^2(q^2-6q+17)}{2^7 \cdot 3}(Y^3Z^2+Y^2Z^3) \right) X^{q-4}, \end{aligned}$$

plus terms involving Y^iZ^j with $i+j \geq 6$.

We note that if we set $Z = Y$ in either of these polynomials we get the first few terms of $W_{C_{1,2}}(X,Y)$,

$$X^{q+1} + (q-1)\binom{q+1}{4}Y^4X^{q-3} + (q-1)(q-4)\binom{q+1}{5}Y^5X^{q-4} + O(Y^6).$$

We note that these first two nonzero coefficients correspond to $q-1$ times the number of collections 4 points and $(q-1)(q-4)$ times the number of collections of 5 points of $\mathbb{P}^1(\mathbb{F}_q)$, respectively. We will give a similar kind of geometric interpretation for the low-weight coefficients $\mathrm{QR}_{C_{1,2}^\perp}(X,Y,Z)$. This involves the number of $\mathbb{F}_q$-points on certain curves in $\mathbb{P}^2(\mathbb{F}_q)$ and $\mathbb{P}^3(\mathbb{F}_q)$.

Suppose that we have a weight 4 codeword $C_{1,2}^\perp$. This is equivalent to four points $\alpha, \beta, \gamma, \delta$ and four coefficients $r_1, r_2, r_3, r_4 \neq 0$, such that

$$r_1g(\alpha) + r_2g(\beta) + r_3g(\gamma) + r_4g(\delta) = 0$$

for all quadratic polynomials $g(x,y) = ax^2+bxy+cy^2$. Up to scalar multiplication we may suppose that $r_4 = 1$. There exists a unique automorphism of $\mathbb{P}^1(\mathbb{F}_q)$ that sends (α,β,γ) to $(\alpha',\beta',\gamma') = ([0:1],[1:1],[1:0])$. This sends δ to another point that we

call $\delta' = [1 : u]$ for $u \in \mathbb{F}_q,\ u \neq 0, 1$. We have $g(\alpha') = c,\ g(\beta') = a + b + c,\ g(\gamma') = a$ and $g(\delta') = cu^2 + bu + a$.

The linear combination of these values coming from the weight 4 codeword can be expressed as

$$(1 + r_3 + r_2)a + (u + r_2)b + (u^2 + r_2 + r_1)c.$$

In order for this expression to vanish for all values of a, b, c we must have $r_2 = -u$. Now the a coefficient vanishes if and only if $r_3 = u - 1$. Finally, the c coefficient vanishes if and only if $r_1 = -u(u - 1)$. Therefore, the nonzero coordinates of a weight 4 codeword are given by $(\omega, -u\omega, (u - 1)\omega, -u(u - 1)\omega)$, where $\omega \in \mathbb{F}_q^*$. We immediately see that an even number of these coefficients are squares, since their product is obviously a square. Therefore, determining the $X^{q-3}Y^4$ coefficient of $\mathrm{QR}_{C_{1,2}}(X, Y, Z)$ is equivalent to determining the number of $u \in \mathbb{F}_q \setminus \{0, 1\}$ for which $-u$ and $u - 1$ are simultaneously squares.

Suppose $-u$ is a nonzero square in $\mathbb{F}_q^*$. Then $u + x^2 = 0$ for some $x \in \mathbb{F}_q^*$. Suppose that $u - 1$ is also a nonzero square. Then $y^2 - u + 1 = 0$ for some $y \in \mathbb{F}_q^*$. This implies $x^2 + y^2 + 1 = 0$ in $\mathbb{F}_q$. We consider the homogenization of this polynomial, $x^2 + y^2 + z^2 = 0$, a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$. This conic has $q + 1$ rational points. When $-u$ and $u - 1$ are nonzero squares there are two distinct choices for the value of x and two distinct choices for the value of y, leading to 4 distinct points of this conic. There are two rational points with $x = 0$ and two rational points with $y = 0$ if and only if the characteristic of $\mathbb{F}_q$ is 1 modulo 4. We consider the points with $z = 0$. Again, there are two of these if and only if the characteristic of $\mathbb{F}_q$ is 1 modulo 4. Combining these observations shows that there are $\frac{q+1}{4}$ values $u \in \mathbb{F}_q \setminus \{0, 1\}$ when the characteristic of $\mathbb{F}_q$ is 3 modulo 4 and $\frac{q-5}{4}$ such values when the characteristic of $\mathbb{F}_q$ is 1 modulo 4 for which $-u$ and $u - 1$ are simultaneously squares. We use this fact to recover the X^{q-3} coefficient of $\mathrm{QR}_{C_{1,2}^{\perp}}(X, Y, Z)$.

We can perform a similar kind of analysis on weight 5 codewords. Again, a unique projective automorphism takes the first three of these points to the $(\alpha', \beta', \gamma')$ of the previous example, and the last two points are $\delta' = [1 : u]$ and $\epsilon' = [1 : v]$, where $u \neq v$ and $u, v \notin \{0, 1\}$. This gives $g(\delta') = cu^2 + bu + a$ and $g(\epsilon') = cv^2 + cv + a$. Up to scalar multiplication we can suppose $r_5 = 1$. For convenience, let $r_4 = \rho$.

In order for the b coefficient to vanish we must have $r_3 = -(\rho u + v)$. If the a coefficient vanishes then $r_2 = \rho u + v - \rho - 1 = \rho(u - 1) + (v - 1)$. Finally, if the c coefficient vanishes then $r_1 = v(1 - v) + \rho u(1 - u)$.

For fixed u, v neither equal to $0, 1$ there are exactly $q-4$ values of ρ so that each of r_1, r_2, r_3, ρ are nonzero. If $r_3 \neq 0$ then $\rho \neq -vu^{-1}$. If $r_2 \neq 0$ then $\rho \neq -(v-1)(u-1)^{-1}$. This inverse exists because $u, v \neq 1$. Also, $vu^{-1} = -(v - 1)(u - 1)^{-1}$ implies $u = v$. Since this is not the case, these two conditions eliminate distinct possibilities for ρ. Finally, if $r_1 \neq 0$ then $\rho \neq -v(1 - v)u^{-1}(1 - u)^{-1}$. Since $u \neq v$, we have $vu^{-1} \neq 1$ and $(1 - v)(1 - u)^{-1} \neq 1$, so this condition on ρ does not coincide with either of the earlier two conditions. Therefore, for any fixed u, v there are three values in $\mathbb{F}_q^*$ that ρ cannot take, giving $q - 4$ possibilities.

We can also interpret this factor of $q - 4$ as follows. Given two distinct vectors $\alpha = (r_{1,1}, r_{2,1}, r_{3,1}, \rho_r, 1)$ and $\beta = (r_{1,2}, r_{2,2}, r_{3,2}, \rho_2, 1)$ with $\rho_1 \neq \rho_2$ satisfying the conditions of the above paragraph and with no coordinates equal to zero, expressing the coordinates in terms of ρ_1, ρ_2, u and v it is easy to see that no $r_{1,i} = r_{2,i}$. So, taking $a\alpha + b\beta$ gives a 2-dimensional subspace of $\mathbb{F}_q^5$ with $q^2 - 1$ nonzero vectors. Projectivizing gives a $\mathbb{P}^1(\mathbb{F}_q)$ of 5-tuples that are given by $\beta, \alpha + i\beta$ where $i \in \{0, 1, \ldots, q - 1\}$. None of these vectors has more than one coordinate equal to zero so it is clear that there are $(q + 1) - 5 = q - 4$ of these vectors that have all nonzero coordinates. This gives the $q - 4$ values of ρ described above.

This gives $(q-1)(q-4)$ times the number of collections of five collinear points dual codewords, and we verify that this is in fact the number of codewords of weight 5 of the dual of the code of quadrics on $\mathbb{P}^1(\mathbb{F}_q)$.

Suppose we have chosen some u, v, ρ so that r_1, r_2, r_3, r_4, ρ are nonzero and that give a weight 5 element c of $C_{1,2}^{\perp}$. This c contributes $X^{q-4}Y^iZ^{5-i}$ to the weight enumerator for some i. The value of i depends on how many of the elements of the set $\{\rho, -(\rho u + v), \rho(u-1) + (v-1), v(1-v) + \rho u(1-u)\}$ are simultaneously squares. We could investigate this question with the strategy used for the discussion of weight 4 codewords, but this involves some intricate work. It is far easier to use the MacWilliams theorem to obtain these types of results.

For $C_{2,2}^{\perp}$ and $C_{1,2}^{\perp}$ we saw that the product of the coordinates of a codeword of minimum weight is always a non-zero square. Minimum weight codewords have support given by four collinear points. The argument given above generalizes to the code $C_{n,2}$.

Proposition 36. *Let $C_{n,2}$ be the code of quadrics on $\mathbb{P}^n(\mathbb{F}_q)$. The minimum weight codewords of $C_{n,2}^{\perp}$ have weight 4 and the product of the coordinates of any such codeword is a square in $\mathbb{F}_q^*$.*

In fact, this type of behavior occurs much more generally. We will see in the next section that a similar statement holds for the code $C_{1,4}$ consisting of quartics on $\mathbb{P}^1(\mathbb{F}_q)$. In Chapter 4 we will prove a similar statement for the code of homogeneous quartics restricted to a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$.

A nice property of the quadratic residue weight enumerator of the code of homogeneous polynomials of weight $2k$ on $\mathbb{P}^n(\mathbb{F}_q)$ is that it does not depend on the choices of affine representatives for the points of $\mathbb{P}^n(\mathbb{F}_q)$. Scaling a point $[x_0 : \cdots : x_n]$ by some $\alpha \in \mathbb{F}_q^*$ gives

$$F_{2k}(\alpha x_0, \ldots, \alpha x_n) = \alpha^{2k} F_{2k}(x_0, \ldots, x_n).$$

If the degree of F is odd, then scaling a point by a non-square $\alpha \in \mathbb{F}_q^*$ can change whether F takes a square or a non-square value at a given point. Therefore, we will not consider quadratic residue weight enumerators of codes coming from homogeneous polynomials of odd degree.

Over the next few sections, we turn to the next simplest case, the quadratic residue weight enumerator for $C_{1,4}$, the code of quartics on $\mathbb{P}^1(\mathbb{F}_q)$. This is significantly more difficult than the case of quadrics because here we first encounter varieties that are not rational.

4. Cones over Singular Quartics on $\mathbb{P}^1(\mathbb{F}_q)$

Let $C_{1,4}$ denote the 5-dimensional code of homogeneous quartics on $\mathbb{P}^1(\mathbb{F}_q)$. We can determine the Hamming weight enumerator of $C_{1,4}$ by noting that there are only a few possibilities for the factorization of a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$ over $\overline{\mathbb{F}}_q$ and counting the number of quartics that give rise to such a factorization. These possibilities are: the fourth power of a linear form defined over $\mathbb{F}_q$, the cube of a linear form defined over $\mathbb{F}_q$ times a distinct linear form, the product of the squares of two distinct linear forms defined over $\mathbb{F}_q$, the product of the square of one linear form defined over $\mathbb{F}_q$ and two other distinct linear forms defined over $\mathbb{F}_q$, the product of four distinct linear forms defined over $\mathbb{F}_q$, the product of four Galois-conjugate forms defined over $\mathbb{F}_{q^4}$, the product of three Galois-conjugate linear forms defined over $\mathbb{F}_{q^3}$ and one linear form defined over $\mathbb{F}_q$, the square of a product of two Galois-conjugate linear forms defined over $\mathbb{F}_{q^2}$, the product of two Galois-conjugate linear forms defined over $\mathbb{F}_{q^2}$ with the square of a linear form defined over $\mathbb{F}_q$, the product of two Galois-conjugate linear forms defined over $\mathbb{F}_{q^2}$ with the product of two distinct linear forms defined over $\mathbb{F}_q$, and the product of two distinct pairs of Galois-conjugate linear forms defined over $\mathbb{F}_{q^2}$. One can see how counting the number of quartics of each of these types is a straightforward, although quite tedious, way to compute $W_{C_{1,4}}(X, Y)$.

Proposition 37. *We have*

$$\begin{aligned} W_{C_{1,4}}(X,Y) &= X^{q+1} + \frac{(q-1)^2(q-2)q(q+1)}{24}X^4Y^{q-3} \\ &+ \frac{(q-1)^2q(q+1)}{2}X^3Y^{q-2} + \frac{(q-1)q(q+1)(q^2-q+6)}{4}X^2Y^{q-1} \\ &+ \frac{(q-1)(q+1)(2q^3+3q^2-5q+6))}{6}XY^q \\ &+ \frac{(q-1)^2q(3q^2+q+2)}{8}Y^{q+1}. \end{aligned}$$

There is a much more general way to understand the Hamming weight enumerators for the codes $C_{1,n}$ of homogeneous degree n forms on $\mathbb{P}^1(\mathbb{F}_q)$ that is explained in [**20**]. These codes are known as classical Goppa codes and come from line bundles on $\mathbb{P}^1$. They are directly related to the famous Reed-Solomon codes, which can be recovered by deleting a coordinate. They are *maximum distance separable*, denoted MDS, which means that their minimum distance gives equality for the Singleton bound.

Proposition 38 (Singleton Bound)**.** *Let $C \subset \mathbb{F}_q^N$ be a linear code with minimum distance d. Then*

$$|C| \leq q^{N-d+1}.$$

See Section 10 of Chapter 1 of [**34**] for a proof of this simple fact.

The weight enumerator of an MDS code $C \subset \mathbb{F}_q^N$ is determined by its minimum distance d and its length N. We give the description of $W_C(X,Y)$ given in [**20**]. Let $d = n - h + 1$ be the minimum weight of a nonzero codeword of C. Let $w \geq d$. The number of words of weight w is

$$\binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}.$$

See Section 3 of Chapter 11 of [**34**] for a proof. We note that this matches the computation above for $C_{1,4}$ and the earlier computation for $C_{1,2}$.

We determine the first few coefficients $W_{C_{1,4}}(X,Y)$ by applying the MacWilliams theorem. The dimension of this code is 5 and we see that $q^{-5}W_{C_{1,4}}(X+(q-1)Y, X-Y)$ equals

$$\begin{aligned} & X^{q+1} + (q-1)\left(\binom{q+1}{6}X^{q-5}Y^6 + (q-6)\binom{q+1}{7}X^{q-6}Y^7\right. \\ + \quad & (q^2-7q+21)\binom{q+1}{8}X^{q-7}Y^8 + (q^3-8q^2+28q-56)\binom{q+1}{9}X^{q-8}Y^9 \\ + \quad & \left.(q^4-9q^3+36q^2-84q+126)\binom{q+1}{10}X^{q-9}Y^{10}\right) + O(Y^{11}). \end{aligned}$$

A major goal of this chapter is to compute $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$. It is easy to see that this is related to counting points on varieties given by $w^2 = f_4(x,y)$, which are homogeneous quartics in the weighted projective space $\mathbb{P}(2,1,1)$. Every homogeneous quartic of this type takes a nonzero value at the singular point of this weighted projective space. We see that computing the specialization $\mathrm{QR}_{C_{1,4}}(X,X^2,1)$ is equivalent to determining the weight enumerator of the nonlinear code of size q^5 coming from homogeneous quartics of the form $w^2 = f_4(x,y)$ on $\mathbb{P}(2,1,1)$. We will return to this correspondence in Chapter 4.

A quartic on $\mathbb{P}^1(\mathbb{F}_q)$ is singular if and only if it has a double root. For a singular quartic $f_4(x,y)$ the variety $w^2 = f_4(x,y)$ is also singular and it is easy to count its $\mathbb{F}_q$-points. When $f_4(x,y)$ is nonsingular, then the Riemann-Hurwitz formula implies that the variety $w^2 = f_4(x,y)$ is a smooth genus 1 curve. Hasse's theorem implies that every genus 1 curve defined over $\mathbb{F}_q$ has an $\mathbb{F}_q$-rational point. We recall that a genus 1 curve with a rational point is an elliptic curve.

Before turning to the theory of elliptic curves over finite fields, we give some results that we will later need when computing $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ about varieties of the form $w^2 = f_4(x,y)$ where $f_4(x,y,)$ is singular.

Proposition 39. *Let $g(x,y)$ be an irreducible quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_q)$ with two Galois-conjugate roots defined over $\mathbb{F}_{q^2}$. For each non-isomorphic quartic on*

$\mathbb{P}^1(\mathbb{F}_q)$, *we list its the number of roots, the number of quartics* $f_4(x,y)$ *of this type, and the number of* $\mathbb{F}_q$*-points of the variety* $w^2 = f_4(x,y)$*:*

Type of Equation	*# Quartics*	*# Roots*	*# points on* $w^2 = f_4(x,y)$
$\eta(x-\alpha y)^4$	$\frac{(q-1)(q+1)}{2}$	1	$1+2q$
$\delta(x-\alpha y)^4$	$\frac{(q-1)(q+1)}{2}$	1	1
$\eta(x-\alpha y)^3(x-\beta y)$	$\frac{(q-1)q(q+1)}{2}$	2	$q+1$
$\delta(x-\alpha y)^3(x-\beta y)$	$\frac{(q-1)q(q+1)}{2}$	2	$q+1$
$\eta(x-\alpha y)^2(x-\beta y)^2$	$\frac{(q-1)q(q+1)}{4}$	2	$2q$
$\delta(x-\alpha y)^2(x-\beta y)^2$	$\frac{(q-1)q(q+1)}{4}$	2	2
$\eta(x-\alpha y)^2(x-\beta y)(x-\gamma y)$	$\frac{(q-1)^2q(q+1)}{4}$	3	$q+1\pm 1$
$\delta(x-\alpha y)^2(x-\beta y)(x-\gamma y)$	$\frac{(q-1)^2q(q+1)}{4}$	3	$q+1\mp 1$
$\eta(x-\alpha y)^2 g(x,y)$	$\frac{(q-1)^2q(q+1)}{4}$	1	$q+1\pm 1$
$\delta(x-\alpha y)^2 g(X,Z)$	$\frac{(q-1)^2q(q+1)}{4}$	1	$q+1\mp 1$
$\eta g(x,y)^2$	$\frac{(q-1)^2q}{4}$	0	$2(q+1)$
$\delta g(x,y)^2$	$\frac{(q-1)^2q}{4}$	0	0

where η *is any nonzero square in* $\mathbb{F}_q^*$ *and* δ *is any non-square in* $\mathbb{F}_q^*$*.*

Let $\mathrm{QR}^{sing}_{C_{1,4}}(X,Y,Z)$ *denote the Hamming weight enumerator form codewords of this form. Then* $\mathrm{QR}^{sing}_{C_{1,4}}(X,Y,Z)$ *is given by*

$$\begin{aligned} & X^{q+1} + \frac{(q-1)(q+1)}{2} X(Y^q + Z^q) + (q-1)\frac{q(q+1)}{2} X^2 Y^{\frac{q-1}{2}} Z^{\frac{q-1}{2}} \\ + \quad & \frac{(q-1)q(q+1)}{4} X^2(Y^{q-1} + Z^{q-1}) + \frac{(q-1)^2 q(q+1)}{4} X^3(Y^{\frac{q-1}{2}} Z^{\frac{q-3}{2}} + Y^{\frac{q-3}{2}} Z^{\frac{q-1}{2}}) \\ + \quad & \frac{(q-1)^2 q(q+1)}{4} X(Y^{\frac{q+1}{2}} Z^{\frac{q-1}{2}} + Y^{\frac{q-1}{2}} Z^{\frac{q+1}{2}}) + \frac{(q-1)^2 q}{4}(Y^{q+1} + Z^{q+1}). \end{aligned}$$

We note that there is a slight notational difficulty. The linear form that vanishes at $[x:y] = [0:1]$ cannot actually be expressed as $x - \alpha y$ for $\alpha \in \mathbb{F}_q$, but up to scalar multiplication all other linear forms can.

Proof. We note that $f(x,y)$ and its twist by a quadratic non-square, $\delta f(x,y)$, must vanish at the same set of r points, and on the other $(q+1) - r$ points of $\mathbb{P}^1(\mathbb{F}_q)$ exactly one of $f(x,y)$ and $\delta f(x,y)$ takes a square value. Therefore the total number of points on a curve plus the number of points on its twist is $2(q+1)$. Given a monic quartic, we can multiply by any of the $\frac{q-1}{2}$ nonzero squares and get a curve isomorphic to this one, or by any of the $\frac{q-1}{2}$ nonzero non-squares to get a twist of this curve.

We first consider quartics vanishing to order four at a single point of $\mathbb{P}^1(\mathbb{F}_q)$. At any of the other q points of $\mathbb{P}^1(\mathbb{F}_q)$ it takes a nonzero square value.

A polynomial that vanishes to order three but not higher at a given point must vanish at one other point, and is isomorphic to $(x - \alpha y)^3(x - \beta y)$. There are $q+1$ choices for the first factor and q for the second. We want to determine how often $(x - \alpha y)(x - \beta y)$ is a square. We do this by counting points on the curve defined by $w^2 = (x - \alpha y)(x - \beta y)$ on $\mathbb{P}^2(\mathbb{F}_q)$. This is a smooth conic, so it has $q+1$ $\mathbb{F}_q$-points.

A quartic vanishing to order two at two distinct $\mathbb{F}_q$-points is isomorphic to one of the form $(x - \alpha y)^2(x - \beta y)^2$ with $\alpha \neq \beta$. There are $\frac{(q+1)q}{2}$ to pick two of the $q+1$

factors of this form. This quartic evaluates to a square on the $q-1$ points where it does not vanish.

A quartic vanishing to order two at one $\mathbb{F}_q$-point and vanishes at two other $\mathbb{F}_q$-points is isomorphic to a quartic of the form $(x-\alpha y)^2(x-\beta y)(x-\gamma y)$. There are $\frac{(q+1)q(q-1)}{2}$ ways to choose these three factors. We consider the number of points on $w^2=(x-\alpha y)^2(x-\beta y)(x-\gamma y)$ in $\mathbb{P}(2,1,1)$. We have already seen that $w^2=(x-\beta y)(x-\gamma y)$ has $q+1$ points. Therefore, the above equation has $q+1\pm 1$ solutions, depending on whether $(x-\beta y)(x-\gamma y)$ takes a square value at the zero of $(x-\alpha y)$.

A quartic vanishing to order two at one $\mathbb{F}_q$-point and not vanishing on any other $\mathbb{F}_q$-point is isomorphic to $(x-\alpha y)^2 g(x,y)$, where $g(x,y)$ is a quadratic polynomial with Galois-conjugate roots. There are $\frac{q(q-1)}{2}$ such quadratic polynomials. We consider the variety $w^2=(x-\alpha y)^2 g(x,y)$ in $\mathbb{P}(2,1,1)$. We first consider the conic $w^2=g(x,y)$ in $\mathbb{P}^2(\mathbb{F}_q)$. This plane conic is nonsingular, so it has $q+1$ points. We now see that $y^2=(x-\alpha y)^2 g(x,y)$ has either $q+2$ or q points depending on whether $g(x,y)$ takes a square value at the zero of $x-\alpha y$.

For the last two rows of this table, we note that $g(x,y)^2$ does not vanish at any $\mathbb{F}_q$-points, but takes a square value at each of them.

□

One nice check that the counts for the singular quartics is correct is that if we sum the second column and 1 more for the zero quartic, here we get $q^4+q^3-q^2$, which is exactly $q^5-(q-1)^2q^2(q+1)$, the number of nonsingular quartics on $\mathbb{P}^1(\mathbb{F}_q)$.

5. Elliptic Curves over Finite Fields and $C_{1,4}$

In order to determine $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$ we need only count $\mathbb{F}_q$-points on genus 1 curves given by $w^2=f_4(x,y)$ where $f_4(x,y)$ is a homogeneous quartic with no double root.

In this section we review the classical theory of elliptic curves over finite fields. We have seen that these double covers of $\mathbb{P}^1(\mathbb{F}_q)$ branched at the roots of a quartic $f_4(x, y)$ give genus 1 curves, so our first goal is to determine how many points such a curve can have.

Theorem 40 (Hasse)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$\#E(\mathbb{F}_q) = (q + 1) - t,$$

where $|t| \leq 2\sqrt{q}$.

See Section 1 of Chapter 5 of [**43**] for a proof.

Hasse's theorem shows that the number of points on an elliptic curves over a finite field lies in a rather restricted range around the central value $q + 1$. A natural question to ask is: For fixed q, which points in this range occur as the number of points of an elliptic curve E defined over $\mathbb{F}_q$?

Theorem 41 (Deuring)**.** *Let $t \in \mathbb{Z}$ satisfy $|t| \leq 2\sqrt{q}$ and suppose that $t \nmid q$. Then there exists an elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$.*

See [**14**] or Chapter 13 of [**30**] for a proof. The main idea is to consider the possible endomorphism rings of E over $\mathbb{F}_q$. We recall that the endomorphism ring of an elliptic curve E defined over $\overline{\mathbb{Q}}$ is either $\mathbb{Z}$ or an order in an imaginary quadratic number field, and in the latter case we say that E has complex multiplication. The situation over finite fields is different. The endomorphism ring of an elliptic curve E defined over $\mathbb{F}_q$ is either an order in an imaginary quadratic field, or a maximal order in a quaternion algebra. In the latter case the curve is supersingular. Deuring's proof relies on considering all of the possibilities for the endomorphism ring of an elliptic curve E defined over $\mathbb{F}_q$ with $q + 1 - t$ points and determining how many times each occurs. A more refined version of this result is stated by Schoof in [**40**], which follows Deuring's original ideas and related work of Waterhouse [**14, 52**].

We will use Schoof's result that counts the number of isomorphism classes of elliptic curves with a given number of points. We note that if $\#E(\mathbb{F}_q) = q+1-t$ then the quadratic twist E' of such a curve satisfies $j(E) = j(E')$ and $\#E'(\mathbb{F}_q) = q+1+t$. Suppose that p is a prime with $q = p^k$. We recall some notation about class numbers from [**40**].

Definition. *Let $\Delta \in \mathbb{Z}_{<0}$ with $\Delta \equiv 0, 1 \pmod 4$. Let*

$$B(\Delta) = \left\{aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y] : \ a > 0 \ \text{ and } b^2 - 4ac = \Delta\right\}$$

denote the set of positive definite binary quadratic forms of discriminant Δ and let

$$b(\Delta) = \left\{aX^2 + bXY + cY^2 \in B(\Delta) : \ \gcd(a,b,c) = 1\right\}$$

denote the set of primitive forms of discriminant Δ. There is an action of $\mathrm{SL}_2(\mathbb{Z})$ on $B(\Delta)$ given as follows. For $f = aX^2 + bXY + cY^2 \in B(\Delta)$ and $\sigma = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, let

$$f \circ \sigma = a(rX + sY)^2 + b(rX + sY)(tX + uY) + c(tX + uY)^2.$$

One can check that his action respects the set $b(\Delta)$ and that there are only finitely many $\mathrm{SL}_2(\mathbb{Z})$-orbits in $B(\Delta)$.

Definition. *Let $N(t)$ denote the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$.*

Let $h(\Delta) = |b(\Delta)/\mathrm{SL}_2(\mathbb{Z})|$ denote the form class number of the discriminant Δ. We define the Kronecker class number as

$$H(\Delta) = \sum_d h\left(\frac{\Delta}{d^2}\right),$$

where d runs over $d \in \mathbb{Z}_{>0}$ for which $d^2 \mid \Delta$ and $\frac{\Delta}{d^2} \equiv 0$ or $1 \pmod 4$.

The weight enumerator of $C_{1,4}$ involves the size of the automorphism groups of elliptic curves E over $\mathbb{F}_q$. For most values $k \in \mathbb{F}_q$ there are exactly 2 isomorphism classes of curves with j-invariant k. However, it is possible that more than 2 isomorphism classes have j-invariant 0 or 1728. The following result focuses on these more complicated j-invariants. This is the main place in this thesis where we use the assumption that the characteristic of $\mathbb{F}_q$ is not equal to 3.

Proposition 42. *Suppose $q = p^f$ with $p \neq 2, 3$.*

(1) If $\left(\frac{-3}{q}\right) \neq 1$, then there are two isomorphism classes of elliptic curves over $\mathbb{F}_q$ with j-invariant 0.

(2) If $\left(\frac{-3}{q}\right) = 1$, then there are six isomorphism classes of elliptic curves over $\mathbb{F}_q$ with j-invariant 0.

(a) If $p \equiv 2 \pmod 3$, then there are two classes each with $q+1 \pm \sqrt{q}$ points, and one class each with $q + 1 \pm 2\sqrt{q}$ points.

(b) If $p \equiv 1 \pmod 3$, let (a, b) be any pair of integers with $p \nmid a$ and $a^2 - ab + b^2 = q$. There is one class each with $q + 1 - t$ points for the following six values of t: $\{\pm(2a - b), \pm(a + b), \pm(2b - a)\}$.

(1) If $\left(\frac{-1}{q}\right) \neq 1$, then there are two isomorphism classes of elliptic curves over $\mathbb{F}_q$ with j-invariant 1728.

(2) If $\left(\frac{-1}{q}\right) = 1$, then there are four isomorphism classes of elliptic curves over $\mathbb{F}_q$ with j-invariant 1728.

(a) If $p \equiv 3 \pmod 4$, then there are two classes with $q + 1$ points and one class each with $q + 1 \pm 2\sqrt{q}$ points.

(b) If $p \equiv 1 \pmod 4$, let (a, b) be any pair of integers with $p \nmid a$ and $a^2 + b^2 = q$. There is one class each with $q+1-t$ points for the following four values of t: $\{\pm 2a, \pm 2b\}$.

We recall the well-known fact that an elliptic curve E defined over $\mathbb{F}_q$ is supersingular if and only if it satisfies $\#E(\mathbb{F}_q) = q + 1 - t$ where $t \equiv 0 \pmod{p}$. This is exercise 5.10 in [**43**].

PROOF. The statements about the number of isomorphism classes and about the supersingular curves are from Section 5 of [**40**]. We can determine the number of points on a curve by writing the Frobenius endomorphism φ as an element of the endomorphism ring of the curve and doing a simple calculation.

The elliptic curves of j-invariant 0 that are not supersingular are exactly those with $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[\zeta_3]$, where ζ_3 is a primitive third root of unity. We write $\varphi = a + b\zeta_3$ where $q = a^2 - ab + b^2$, the norm of this endomorphism. We see that

$$\#E(\mathbb{F}_q) = |\varphi - 1| = (a-1)^2 - (a-1)b + b^2 = q + 1 - (2a - b).$$

Switching the role of a and b gives a curve with $q+1-(2b-a)$ points. Since a^2-ab+b^2 is the norm of the element $a + b\zeta_3$ in $\mathbb{Q}[\zeta_3]$, we see that $\zeta_3^k(a + b\zeta_3)$ for $k \in [1, 2]$ have the same norm. For $k = 1$,

$$a\zeta_3 + b\zeta_3^2 = a\zeta_3 + b(-\zeta_3 - 1) = -b + (a - b)\zeta_3.$$

The resulting curve has $q + 1 - (2(-b) - (a - b)) = q + 1 + (a + b)$ points. For $k = 2$,

$$a\zeta_3^2 + \zeta_3^3 b = b - a - a\zeta_3,$$

and the resulting curve has $q + 1 - (2(b - a) + a) = q + 1 - (2b - a)$ points. We also see that replacing φ by $-\varphi$ takes a curve with $q + 1 - t$ points to one with $q + 1 + t$ points. This gives the counts for the number of points of the six isomorphism classes of curves with j-invariant 0.

The curves of j-invariant 1728 that are not supersingular all have $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[i]$ [**40**]. We write $\varphi = a + bi$ where $q = a^2 + b^2$, the norm of this endomorphism.

Therefore, $\#E(\mathbb{F}_q) = |\varphi - 1| = (a-1)^2 + b^2 = q + 1 - 2a$. Switching the role of a and b or replacing φ by $-\varphi$ gives the point counts for these four isomorphism classes.

□

Theorem 4.6 from [**40**] gives the values of $N(t)$.

Theorem 43. *Let $t \in \mathbb{Z}$. Then*

$$\begin{aligned} N(t) = &\quad H(t^2 - 4q) && \text{if } t^2 < 4q \text{ and } p \nmid t; \\ = &\quad H(-4p) && \text{if } t = 0 \\ = &\quad 1 && \text{if } t = 2q \text{ and } p = 2 \\ = &\quad 1 && \text{if } t = 3q \text{ and } p = 3 \end{aligned}$$

if q is not a square, and

$$\begin{aligned} N(t) = &\quad H(t^2 - 4q) && \text{if } t^2 < 4q \text{ and } p \nmid t; \\ = &\quad 1 - \left(\tfrac{-1}{p}\right) && \text{if } t = 0 \\ = &\quad 1 - \left(\tfrac{-3}{p}\right) && \text{if } t^2 = q \\ = &\quad \tfrac{1}{12}\left(p + 6 - 4\left(\tfrac{-3}{p}\right) - 3\left(\tfrac{-1}{p}\right)\right) && \text{if } t^2 = 4q \end{aligned}$$

if q is a square, and $N(t) = 0$ in all other cases.

We now know exactly how many isomorphism classes of curves E over $\mathbb{F}_q$ have $q + 1 - t$ points. Given an elliptic curve E over $\mathbb{F}_q$, there is a homogeneous quartic $f_4(x, y)$ such that $w^2 = f_4(x, y)$ is isomorphic to E. We now need to know how many different quartics give an equation of this form isomorphic to E.

Proposition 44. *Let E be an elliptic curve defined over $\mathbb{F}_q$. The number of homogeneous quartic polynomials $f_4(x, y)$ such that $w^2 = f_4(x, y)$ gives a curve isomorphic*

to E is

$$(q-1)\frac{|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}(E)|} = \frac{(q-1)^2 q(q+1)}{|\mathrm{Aut}(E)|}.$$

PROOF. We will phrase this as a double counting argument. Suppose we begin with an elliptic curve E with $q+1-t$ $\mathbb{F}_q$-rational points. We want to know in how many ways we can write this as $w^2 = f_4(x,y)$, where $f_4(x,y)$ is a quartic polynomial. We recall that there are exactly $q+1-t$ choices of degree two divisor classes on E. The Riemann-Roch theorem implies that a degree 2 divisor has a 2-dimensional space of sections. Choosing a basis for this space of sections gives a degree 2 map to $\mathbb{P}^1(\mathbb{F}_q)$. Taking the inverse image of a point in $\mathbb{P}^1(\mathbb{F}_q)$ recovers the degree two divisor class. The branch points of this map are the roots of this quartic.

Now we want to consider how many maps there are taking a particular equation of the form $w^2 = f_4(x,y)$ to the underlying elliptic curve E. We can recover E with a distinguished identity element and a degree 2 divisor class D directly from this equation. Now we take a map that forgets D, taking (E,D) to E, and note that this map is defined only up to an automorphism of E. Since an automorphism must fix the identity element of E, we multiply $|\mathrm{Aut}(E)|$ by the number of possible choices of identity element, $q+1-t$. Therefore, given E there are

$$\frac{(q+1-t)(q-1)|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}(E)|(q+1-t)} = \frac{(q-1)|\mathrm{PGL}_2(\mathbb{F}_q)|}{|\mathrm{Aut}(E)|}$$

quartics $f_4(x,y)$ with $w^2 = f_4(x,y)$ isomorphic to E. □

In Chapter 6, we will see a similar result when we study genus 1 curves given as $(2,2)$-curves on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. Combining this result with the determination of $N(t)$ and the analysis of singular quartics on $\mathbb{P}^1(\mathbb{F}_q)$ of the previous section gives us everything we need to determine the distribution of point counts for equations of the form $w^2 = f_4(x,y)$.

Proposition 45. *Let $q = p^f$ with $p \neq 2, 3$ and $N(t)$ be the number of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with exactly $q + 1 - t$ points. Let $\mathrm{QR}^S_{C_{1,4}}(X, X^2, 1)$ denote the contribution to $\mathrm{QR}_{C_{1,4}}(X, X^2, 1)$ coming from quartics that do not have a double root.*

Let

$$\mathrm{QR}^{S1}_{C_{1,4}}(X, X^2, 1) = \sum_{t=\lceil -2\sqrt{q} \rceil}^{\lfloor 2\sqrt{q} \rfloor} N(t) \frac{(q-1)^2 q(q+1)}{2} X^{q+1-t}.$$

If $\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right) = -1$, then $\mathrm{QR}^S_{C_{1,4}}(X, X^2, 1) = \mathrm{QR}^{S1}_{C_{1,4}}(X, X^2, 1)$.

If $p \equiv 1 \pmod 3$, let (a, b) be any pair of integers with $p \nmid a$ and $a^2 - ab + b^2 = q$. Then we define

$$P_0(X) = \sum_{t' \in T_0} \frac{(q-1)^2 q(q+1)}{3} X^{q+1-t'}$$

where $T_0 = \{\pm(2a - b), \pm(a + b), \pm(2b - a)\}$.

If $p \equiv 2 \pmod 3$ and f is even, then we define

$$P_0(X) = \frac{(q-1)^2 q(q+1)}{3} \left(X^{q+1-2\sqrt{q}} + X^{q+1+2\sqrt{q}} + 2X^{q+1-\sqrt{q}} + 2X^{q+1+\sqrt{q}} \right).$$

Otherwise, let $P_0(X) = 0$.

If $p \equiv 1 \pmod 4$, let (a, b) be any pair of integers with $p \nmid a$ and $a^2 + b^2 = q$. Then we define

$$P_{1728}(X) = \frac{(q-1)^2 q(q+1)}{4} \left(X^{q+1-(2a)} + X^{q+1+(2a)} + X^{q+1-(2b)} + X^{q+1+(2b)} \right).$$

If $p \equiv 3 \pmod 4$ and f is even, we let

$$P_{1728}(X) = \frac{(q-1)^2 q(q+1)}{4} \left(X^{q+1-2\sqrt{q}} + X^{q+1+2\sqrt{q}} + 2X^{q+1} \right).$$

Otherwise let $P_{1728}(X) = 0$.

We have

$$\mathrm{QR}^S_{C_{1,4}}(X, X^2, 1) = \mathrm{QR}^{S1}_{C_{1,4}}(X, X^2, 1) - P_0(X) - P_{1728}(X).$$

This matches our explicit computation for small values of q. If the characteristic of $\mathbb{F}_q$ is 3 then j-invariant 0 and 1728 coincide and we must be more careful in studying curves with more than two automorphisms. In future work, we would like to adapt this statement to deal with this case.

Later in this chapter we will homogenize this to a polynomial of degree q^3+q^2+q in X and Y and investigate what happens under the linear transformation of the classical MacWilliams identity.

We have not quite computed $\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$. For these terms coming from genus 1 curves we need to separate equations of the form $w^2 = f_4(x,y)$ by the number of $\mathbb{F}_q$-rational roots of $f_4(x,y)$.

6. The Quadratic Residue Weight Enumerator for Quartics on $\mathbb{P}^1(\mathbb{F}_q)$

In this section we adapt the previous computation of $\mathrm{QR}^S_{C_{1,4}}(X,X^2,1)$ to determine $\mathrm{QR}^S_{C_{1,4}}(X,Y,Z)$. The main problem we need to solve is the following. Suppose that there are M smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has exactly $q+1-t$ $\mathbb{F}_q$-points. Let M_k be the number of these quartics with k $\mathbb{F}_q$-rational roots. We know that $M_0 + M_1 + M_2 + M_3 + M_4 = M$, but we need the individual values of these terms. If a quartic $f_4(x,y)$ defined over $\mathbb{P}^1(\mathbb{F}_q)$ has 4 distinct roots and 3 of them are $\mathbb{F}_q$-rational, then because the roots are distinct and the coefficients of the quartic are in $\mathbb{F}_q$, the fourth root is also $\mathbb{F}_q$-rational. Therefore, $M_3 = 0$. This lets us determine M_1.

Lemma 46. *Suppose that $q+1-t$ is odd and that there are M smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has exactly $q+1-t$ $\mathbb{F}_q$-points. Then $M_1 = M$ and $M_0 = M_2 = M_4 = 0$.*

Suppose that $q+1-t$ is even and that there are M smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has exactly $q+1-t$ $\mathbb{F}_q$-points. Then $M_1 = 0$.

PROOF. The number of $\mathbb{F}_q$-rational points of $w^2 = f_4(x, y)$ is the number of $\mathbb{F}_q$-rational roots of $f_4(x, y)$ plus twice the number of points $[x_1 : y_1]$ of $\mathbb{P}^1(\mathbb{F}_q)$ for which $f_4(x_1, y_1)$ is a nonzero square value. Therefore, if $q + 1 - t$ is odd, then the number of roots of $f_4(x, y)$ is odd. If $q + 1 - t$ is even, then the number of roots of $f_4(x, y)$ is even. □

We must now suppose that $q + 1 - t$ is even and determine how these M quartics break up into those that have $0, 2$, and 4 $\mathbb{F}_q$-rational roots. We first note that for an elliptic curve in affine Weierstrass form $y^2 = f(x) = x^3 + ax + b$, the roots of the homogeneous quartic $y(x^3 + axy^2 + by^3)$ are exactly the 2-torsion points of E. When we consider curves given by $w^2 = f_4(x, y)$, a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$ there is a similar correspondence between roots of $f_4(x, y)$ and 2-torsion points of E.

Lemma 47. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose that there are M quartics $f_4(x, y)$ with $w^2 = f_4(x, y)$ isomorphic to E. Let $M = M_0 + M_2 + M_4$, where M_k is the number of quartics with k $\mathbb{F}_q$-rational roots.*

(1) If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$ then $M_0 = M_2 = \frac{M}{2}$ and $M_4 = 0$.
(2) If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then $M_0 = \frac{3M}{4}, M_2 = 0$, and $M_4 = \frac{M}{4}$.

PROOF. Given an elliptic curve E defined over $\mathbb{F}_q$ we describe how to find all quartics $f_4(x, y)$ with $w^2 = f_4(x, y)$ isomorphic to E. The Riemann-Roch theorem implies that a degree 2 divisor on E has a 2-dimensional space of sections. Given a degree 2 divisor on E, choosing a basis for this space of sections gives a degree 2 map to $\mathbb{P}^1(\mathbb{F}_q)$. We take this divisor to be $(O) + (P)$, where O is the identity element of the group law of E and P is another $\mathbb{F}_q$-rational point of E.

A point $P \in E(\mathbb{F}_q)$ gives a map from E to $\mathbb{P}^1(\mathbb{F}_q)$ given by sections of the divisor $(O) + (P)$. A zero of this quartic corresponds to a point $Q \in E(\bar{\mathbb{F}}_q)$ with $2Q \sim O + P$, or $2Q = P$ in the group law on the curve.

We vary over all choices of P and consider how many Q occur as points with $2Q = P$. If $\#E(\mathbb{F}_q)$ is odd, then the map $P \to 2P$ is an isomorphism, so every P gives exactly one such Q. If $\#E(\mathbb{F}_q)$ is even then there are two possibilities for the group structure of $E(\mathbb{F}_q)[2]$. If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$ then $1/2$ of points of $E(\mathbb{F}_q)$ have 0 preimages under the map $P \to 2P$, and $1/2$ have exactly 2. If $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then $1/4$ of points of $E(\mathbb{F}_q)$ have 4 preimages under the map $P \to 2P$, and $3/4$ have none. □

We now give a criterion to determine the group structure of $E(\mathbb{F}_q)[2]$. We have already seen that $E(\mathbb{F}_q)$ is exactly the set of points fixed by the Frobenius endomorphism φ, or equivalently $\ker(\varphi - 1)$. Therefore, all 2-torsion of E is rational if and only if $E[2] \subseteq E[\varphi - 1]$. This will be a useful characterization when studying curves with j-invariant 0 and 1728. For curves with other j-invariants we use the following result, Lemma 4.8 in [**40**].

Lemma 48. *Let $q = p^f$ where p is prime. Suppose that $t \in \mathbb{Z}$ satisfies $|t| \leq 2\sqrt{q}$. Let $N_{2\times 2}(t)$ be the number of isomorphism classes of elliptic curves E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$.*

(1) If $p \nmid t$ and $t \equiv q + 1 \pmod 4$, then

$$N_{2,2}(t) = H\left(\frac{t^2 - 4q}{4}\right).$$

(2) If $t^2 = q, 2q$, or $3q$, then $N_{2,2}(t) = 0$.

(3) If $t^2 = 4q$ then $N_{2,2}(t) = N(t)$.

(4) Let $t = 0$. If $q \equiv 1 \pmod 4$ then $N_{2,2}(t) = 0$. If $q \equiv 3 \pmod 4$ then $N_{2,2}(t) = h(-p)$.

We now turn to the case where the j-invariant of E is 0 or 1728.

Lemma 49. *Suppose $q = p^f$ and that $\left(\frac{-3}{q}\right) = 1$. Then there are six isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with j-invariant 0.*

(1) If $p \equiv 1 \pmod 3$ *then there exists a pair of integers* (a, b) *with* $p \nmid a$ *and* $a^2 - ab + b^2 = q$. *There is an elliptic* E *of* j*-invariant* 0 *isomorphic to a curve in Weierstrass form* $y^2 = x^3 + a_6$. *Then* $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if and only if* a_6 *is a cube in* $\mathbb{F}_q^*$. *This occurs if and only if* a *is odd and* b *is even.*

(2) When $q \equiv 2 \pmod 3$ *every elliptic curve* E *of* j*-invariant* 0 *has* $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$.

PROOF. The statement about the number of isomorphism classes is part of Proposition 42. Every elliptic curve E of j-invariant 0 is isomorphic to one of the form $y^2 = x^3 + a_6$. This follows from the fact that every elliptic curve over a finite field of characteristic not equal to 2 is isomorphic to one of the form $y^2 = x^3 + a_4x + a_6$, and that $j(E) = 1728\frac{4a_4^3}{4a_4^3+27a_6^2}$. The 2-torsion points of E correspond to the roots of $x^3 + a_6$ in $\mathbb{F}_q$ together with the point at infinity.

When $p \equiv 2 \pmod 3$ the map $x \to x^3$ on $\mathbb{F}_q^*$ is an isomorphism and $x^3 + a_6$ has exactly one root. Therefore $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$.

When $p \equiv 1 \pmod 3$ exactly $\frac{q-1}{3}$ elements $a_6 \in \mathbb{F}_q^*$ are cubes, so the map $x \to x^3$ has three preimages, and the other points have no preimages. So, exactly 1/3 of the quartics $f_4(x, y)$ with $w^2 = f_4(x, y)$ isomorphic to E have four rational 2-torsion points.

The elliptic curves of j-invariant 0 that are not supersingular are exactly those with $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[\zeta_3]$ where ζ_3 is a primitive third root of unity. We have seen above that if we write $\varphi = a + b\zeta_3$ then $|\varphi - 1| = q + 1 - (2a - b)$. Multiplying φ by ζ_3 gives $\varphi = -b + (a - b)\zeta_3$. Multiplying φ by ζ_3^2 gives $\varphi = (b - a) - a\zeta_3$. In each of these cases, we can also replace φ by $-\varphi$. We have $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if $\frac{\varphi-1}{2}$ is in $\mathbb{Z}[\zeta_3]$. If $\varphi = a + b\zeta_3$, this occurs if and only if a is odd and b is even.

□

Lemma 50. *Suppose $q = p^f$ and $\left(\frac{-1}{q}\right) = 1$. Then there are four isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with j-invariant* 1728*.*

(1) If $p \equiv 1 \pmod 4$ then there exists a pair of integers (a, b) with $p \nmid a$ and $q = a^2 + b^2$. Then there is an elliptic E of j-invariant 1728 *isomorphic to a curve in Weierstrass form $y^2 = x^3 - a_4 x$ and $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if a_4 is a square in $\mathbb{F}_q^*$. This occurs if and only if a is odd and b is even.*

(2) If $p \equiv 3 \pmod 4$ and f is even, then any elliptic curve E with j-invariant 1728 *is supersingular and satisfies either $\#E(\mathbb{F}_q) = q + 1$ and $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$, or $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q}$ and $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. This is very similar to the proof of the previous result. The statement about the number of isomorphism classes is part of Proposition 42. The fact that every elliptic curve E of j-invariant 1728 is isomorphic to one of the form $y^2 = x^3 - a_4 x$ follows from the fact that every elliptic curve is isomorphic to one in Weierstrass form, $y^2 = x^3 + a_4 x + a_6$, and that $j(E) = 1728$ if and only $j(E) = 1728$ if and only if $a_4 \neq 0$ and $a_6 = 0$. Now, we see that 2-torsion corresponds to the number of roots of $x^2 - a_4$ in $\mathbb{F}_q$. So $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if a_4 is a square in $\mathbb{F}_q^*$.

We have already seen above that the curves with j-invariant 1728 that are not supersingular satisfy $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[i]$. We write $\varphi = a + bi$ where $q = a^2 + b^2$, the norm of this endomorphism. We see that $\#E(\mathbb{F}_q) = |\varphi - 1| = (a-1)^2 + b^2 = q + 1 - 2a$. We multiply φ by i^k with $k \in [0, 3]$ without changing $|\varphi|$. All of the 2-torsion of E is rational if and only if $\frac{\varphi - 1}{2}$ is an endomorphism of E. This is the case if and only if $a - 1$ and b are both even.

When a curve of j-invariant 1728 is supersingular and has exactly $q + 1$ points, the fact that $q \equiv 1 \pmod 4$ together with Lemma 48 imply that $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$. When $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q}$, Theorem 48 implies that $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\square$

We can now give the main result of this section, the contribution to the quadratic residue weight enumerator from all smooth homogeneous quartics $f_4(x, y)$.

Theorem 51. *Let $q = p^f$ with $p \neq 2, 3$ and $N(t)$ be the number of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with exactly $q + 1 - t$ points and $N_{2,2}(t)$ be the number of these isomorphism classes for which $E(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\mathrm{QR}^S_{C_{1,4}}(X, Y, Z)$ denote the contribution to $\mathrm{QR}_{C_{1,4}}(X, Y, Z)$ coming from quartics that do not have a double root.*

Let

$$\mathrm{QR}^{S1}_{C_{1,4}}(X, Y, Z) = \sum_{\substack{\lceil -2\sqrt{q} \rceil \leq t \leq \lfloor 2\sqrt{q} \rfloor \\ t \equiv 1 \pmod 2}} N(t) \frac{(q-1)^2 q(q+1)}{2} XY^{\frac{q-t}{2}} Z^{\frac{q+t}{2}}$$

$$+ \sum_{\substack{\lceil -2\sqrt{q} \rceil \leq t \leq \lfloor 2\sqrt{q} \rfloor \\ t \equiv 0 \pmod 2}} \Bigg((N(t) - N_{2,2}(t)) \frac{(q-1)^2 q(q+1)}{4} (X^2 Y^{\frac{q-1-t}{2}} Z^{\frac{q-1+t}{2}} + Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}})$$

$$+ N_{2,2}(t) \frac{(q-1)^2 q(q+1)}{8} \left(3X^4 Y^{\frac{q-3-t}{2}} Z^{\frac{q-3+t}{2}} + Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}} \right) \Bigg)$$

If $\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right) = -1$, then $\mathrm{QR}^S_{C_{1,4}}(X, Y, Z) = \mathrm{QR}^{S1}_{C_{1,4}}(X, Y, Z)$.

If $p \equiv 1 \pmod 3$, let (a, b) be any pair of integers with $p \nmid a$ and $a^2 - ab + b^2 = q$. We define $P_0(X, Y, Z, a, b, t)$ for t in the set $T_0 := \{\pm(2a - b), \pm(a + b), \pm(2b - a)\}$. If t is odd, then

$$P_0(X, Y, Z, a, b, t) = \frac{(q-1)^2 q(q+1)}{3} XY^{\frac{q-t}{2}} Z^{\frac{q+t}{2}}.$$

If t is even, a is odd, and b is even,

$$P_0(X, Y, Z, a, b, t) = \frac{(q-1)^2 q(q+1)}{12} \left(3X^4 Y^{\frac{q-3-t}{2}} Z^{\frac{q-3+t}{2}} + Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}} \right).$$

If t is even, and it is not the case that a is odd and b is even,

$$P_0(X, Y, Z, a, b, t) = \frac{(q-1)^2 q(q+1)}{6} \left(X^2 Y^{\frac{q-1-t}{2}} Z^{\frac{q-1+t}{2}} + Y^{\frac{q+1-t}{2}} Z^{\frac{q+1+t}{2}} \right).$$

We define $P_0(X,Y,Z)$ *to be the sum of* $P_0(X,Y,Z,a,b,t)$ *where* t *ranges through the set* T_0.

If $p \equiv 2 \pmod 3$ *and* f *is even, then we define*

$$\begin{aligned}P_0(X,Y,Z) = \frac{(q-1)^2q(q+1)}{6}\Bigg(X^2\Bigg(&Y^{\frac{q-1-2\sqrt{q}}{2}}Z^{\frac{q-1+2\sqrt{q}}{2}} + Y^{\frac{q-1+2\sqrt{q}}{2}}Z^{\frac{q-1-2\sqrt{q}}{2}}\\ &+2\left(Y^{\frac{q-1-\sqrt{q}}{2}}Z^{\frac{q-1+\sqrt{q}}{2}} + Y^{\frac{q-1+2\sqrt{q}}{2}}Z^{\frac{q-1-2\sqrt{q}}{2}}\right)\Bigg)\\ &+Y^{\frac{q+1-2\sqrt{q}}{2}}Z^{\frac{q+1+2\sqrt{q}}{2}} + Y^{\frac{q+1+2\sqrt{q}}{2}}Z^{\frac{q+1-2\sqrt{q}}{2}}\\ &+2\left(Y^{\frac{q+1-\sqrt{q}}{2}}Z^{\frac{q+1+\sqrt{q}}{2}} + Y^{\frac{q+1+2\sqrt{q}}{2}}Z^{\frac{q+1-2\sqrt{q}}{2}}\right)\Bigg).\end{aligned}$$

Otherwise, let $P_0(X,Y,Z) = 0$.

If $p \equiv 1 \pmod 4$, *let* (a,b) *be any pair of integers with* $p \nmid a$ *and* $a^2+b^2 = q$. *Then we define* $P(X,Y,Z,a,b,t)$ *to be*

$$\begin{aligned}&\frac{(q-1)^2q(q+1)}{8}\left(X^2Y^{\frac{q-1-t}{2}}Z^{\frac{q-1+t}{2}} + Y^{\frac{q+1-t}{2}}Z^{\frac{q+1+t}{2}}\right) \text{ if } b \text{ odd and } a \text{ even,}\\ &\frac{(q-1)^2q(q+1)}{16}\left(3X^4Y^{\frac{q-3-t}{2}}Z^{\frac{q-3+t}{2}} + Y^{\frac{q+1-t}{2}}Z^{\frac{q+1+t}{2}}\right) \text{ if } a \text{ odd and } b \text{ even.}\end{aligned}$$

We let

$$\begin{aligned}P_{1728}(X,Y,Z) &:= P(X,Y,Z,a,b,2a) + P(X,Y,Z,a,b,2b)\\ &+ P(X,Y,Z,a,b,-2a) + P(X,Y,Z,a,b,-2b).\end{aligned}$$

If $p \equiv 3 \pmod 4$ *and* f *is even, then*

$$\begin{aligned}P_{1728}(X,Y,Z) &= \frac{(q-1)^2q(q+1)}{4}\left(X^2Y^{\frac{q-1}{2}}Z^{\frac{q-1}{2}} + Y^{\frac{q+1}{2}}Z^{\frac{q+1}{2}}\right)\\ &+ \frac{(q-1)^2q(q+1)}{16}\Bigg(3X^4\left(Y^{\frac{q-3+2\sqrt{t}}{2}}Z^{\frac{q-3-2\sqrt{t}}{2}} + Y^{\frac{q-3-2\sqrt{t}}{2}}Z^{\frac{q-3+2\sqrt{t}}{2}}\right)\\ &+ \left(Y^{\frac{q+1+2\sqrt{t}}{2}}Z^{\frac{q+1-2\sqrt{t}}{2}} + Y^{\frac{q+1-2\sqrt{t}}{2}}Z^{\frac{q+1+2\sqrt{t}}{2}}\right)\Bigg).\end{aligned}$$

We have

$$\mathrm{QR}^{S}_{C_{1,4}}(X,Y,Z) = \mathrm{QR}^{S1}_{C_{1,4}}(X,Y,Z) - P_0(X,Y,Z) - P_{1728}(X,Y,Z).$$

The proof of this theorem comes from carefully applying the previous lemmas. We can combine this result with the computation of $\mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X,Y,Z)$, the contribution from singular quartics above to completely determine the quadratic residue weight enumerator of quartics on $\mathbb{P}^1(\mathbb{F}_q)$, $\mathrm{QR}_{C_{1,4}}(X,Y,Z)$.

We give the example $q = 5$. We have computed

$$\begin{aligned}\mathrm{QR}^{\mathrm{sing}}_{C_{1,4}}(X,Y,Z) &= X^6 + 120\,X^3Y^2Z + 120\,X^3YZ^2 + 30\,X^2Y^4 + 120\,X^2Y^2Z^2 \\ &+ 30\,X^2Z^4 + 12\,XY^5 + 120\,XY^3Z^2 + 120\,XY^2Z^3 + 12XZ^5 \\ &+ 20\,Y^6 + 20\,Z^6.\end{aligned}$$

We also compute that

$$\begin{aligned}\mathrm{QR}^{S}_{C_{1,4}}(X,Y,Z) &= 30\,X^4Y^2 + 30\,X^4Z^2 + 60\,X^2Y^4 + 120\,X^2Y^3Z + 240\,X^2Y^2Z^2 \\ &+ 120\,X^2YZ^3 + 60\,X^2Z^4 + 240\,XY^4Z + 240\,XY^3Z^2 \\ &+ 240\,XY^2Z^3 + 240\,XYZ^4 + 60\,Y^5Z + 210\,Y^4Z^2 \\ &+ 240\,Y^3Z^3 + 210\,Y^2Z^4 + 60\,YZ^5.\end{aligned}$$

The sum of these two terms matches our explicit computation, listing all 5^5 elements of this code and keeping track of how many coordinates of each codeword are 0, nonzero squares, and non-squares.

We focus on a particular term. Consider the contribution to this weight enumerator from smooth quartics $f_4(x,y)$ such that $w^2 = f_4(x,y)$ has $5+1-2 = 4$ $\mathbb{F}_5$-points. We compute that $N(2) = 2$ and $N_{2,2}(2) = 1$. We see that $5 = (-1)^2 + 2^2$, so there is an elliptic curve over $\mathbb{F}_5$ of j-invariant 1728 with $5 + 1 - t = 4$. The isomorphism

class with j-invariant 1728 contributes 120 quartics, and since a is odd and b is even we see that $\frac{1}{4}$ of them have four $\mathbb{F}_q$-rational roots, and $\frac{3}{4}$ have no $\mathbb{F}_q$-rational roots. The other isomorphism class contributes 240 quartics, half of which have two roots, and half of which have no roots. Together these quartics contribute

$$30\,X^4Y^2 + 120\,X^2YZ^3 + 210\,Y^2Z^4.$$

Applying the quadratic residue version of the MacWilliams identity shows that $\mathrm{QR}_{C_{1,4}^{\perp}}(X, Y, Z)$ is equal to

$$\frac{\mathrm{QR}_{C_{1,4}}\left(X + 2(Y+Z), X - Z + \frac{\sqrt{5}-1}{2}(Y-Z), X - Y + \frac{\sqrt{5}-1}{2}(Z-Y)\right)}{5^5},$$

which is $X^6 + 2Y^6 + 2Z^6$.

7. The Quadratic Residue Weight Enumerator of $C_{1,4}^{\perp}$

We would like to find the first few nonzero coefficients of the quadratic residue weight enumerator of $C_{1,4}^{\perp}$. We first consider the related problem of the studying the weight enumerator of cones over elliptic curves given as double covers of $\mathbb{P}^1(\mathbb{F}_q)$ under the MacWilliams transformation. If the curve $w^2 = f_4(x, y)$ in the weighted projective space $\mathbb{P}(2, 1, 1)$ has t $\mathbb{F}_q$-rational points, then the cone over this curve in $\mathbb{P}(2, 1, 1, 1)$ will have $1 + qt$ points. We recall that in the setup of codes from degree 2 del Pezzo surfaces given by equations of the form $w^2 = f_4(x, y, z)$ we do not evaluate at the singular point of the weighted projective space $[1 : 0 : 0 : 0]$. We saw that a quartic $f_4(x, y, z)$ depending only on $[x : y]$ gives a cone with vertex $[w : x : y : z] = [0 : 0 : 0 : 1]$. Changing the cone point does not change the contribution to the weight enumerator from codewords of this form. Therefore, we want to find the contribution to the weight enumerator from the terms of

$$(q^2 + q + 1)X\mathrm{QR}_{C_{1,4}^{\perp}}(X^q, X^{2q}, 1),$$

where we homogenize this polynomial with respect to a variable Y so that it has degree q^3+q^2+q. This polynomial is exactly the $W^{G1}_{C'_{2,4}}(X,Y)$ defined in Chapter 2.

We now need a critical fact about the contribution of $W^{G1}_{C'_{2,4}}(X,Y)$ to the dual code. We first recall a definition from the theory of modular forms.

Definition. *Let Δ denote the unique cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. Let $\tau(q)$ denote the coefficient of the $e^{2\pi izq}$ term of the Fourier expansion of Δ.*

Theorem 52. *Each coefficient of $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y) \pmod{Y^{10}}$ is a polynomial in q. The Y^{10} coefficient of $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ is a polynomial in q plus a polynomial in q times $\tau(q)$.*

This result follows from work of Birch on powers of traces of elliptic curve [**3**]. We will discuss this work at the end of this section.

Supposing that we have established that these coefficients are polynomials in q we can find them by producing these weight enumerators explicitly for many small values of q and using Lagrange interpolation. We note that the degree of any coefficient of $W^{G1}_{C'_{2,4}}(X,Y)$ as a polynomial in q is at most 7, since there are only $(q^2+q+1)q^5$ terms that contribute to the sum. So, the maximum degree in of the Y^j coefficient of $W^{G1}_C(X+(q-1)Y, X-Y)$ is at most 7 plus the degree of $\binom{q^3+q^2+q}{j}$. Therefore, to determine the polynomials of weight up to 9, we need only determine $W^{G1}_C(X+(q-1)Y, X-Y)$ for the first 35 primes larger than 3. As a check on this computation we produce this weight enumerator for all primes less than 350. We want to find the value of $P_1(q)+P_2(q)\tau(q)$ where $P_1(q)$ and $P_2(q)$ are polynomials in q that give the Y^{10} term. By the same reasoning, the degree of each of these polynomials is at most 37.

Proposition 53. *$W^{G1}_C(X+(q-1)Y, X-Y)$ modulo Y^{11} is equal to*

$$(q^3-1)(q^3-q)q\sum_{j=0}^{10}\frac{A_j(q)}{j!}X^{q^3+q^2+q-j}Y^j+O(Y^{11}),$$

where the values of $A_j(q)$ are:

$$
\begin{aligned}
A_0(q) &= 1, \quad A_1(q) = 0, \\
A_2(q) &= (q-1)\big(q^3-q-1\big)q, \\
A_3(q) &= -(q-2)(q-1)^2\big(3\,q^2+4\,q+2\big)q \\
A_4(q) &= \big(2\,q^9-6\,q^8+16\,q^6-36\,q^5+37\,q^4+12\,q^3-30\,q^2-15\,q+18\big)q \\
A_5(q) &= -2(q-2)\big(10\,q^9-25\,q^8-5\,q^7+45\,q^6-47\,q^5+39\,q^4+11\,q^3-48\,q^2-14\,q+24\big)q \\
A_6(q) &= \Big(5\,q^{14}-30\,q^{13}+36\,q^{12}+195\,q^{11}-976\,q^{10}+1675\,q^9-256\,q^8-2630\,q^7+3111\,q^6-1570\,q^5 \\
&\quad +205\,q^4+1240\,q^3-1015\,q^2-770\,q+600\Big)q \\
A_7(q) &= -(q-2)\Big(105\,q^{14}-560\,q^{13}+546\,q^{12}+1995\,q^{11}-7070\,q^{10}+9387\,q^9-133\,q^8-14426\,q^7+13443\,q^6 \\
&\quad -3290\,q^5-273\,q^4+3066\,q^3-4578\,q^2-2052\,q+2160\Big)q \\
A_8(q) &= \Big(14\,q^{19}-140\,q^{18}+392\,q^{17}+1422\,q^{16}-13972\,q^{15}+39969\,q^{14}-28420\,q^{13}-110600\,q^{12} \\
&\quad +335741\,q^{11}-398609\,q^{10}+86072\,q^9+424152\,q^8-587104\,q^7+264278\,q^6+18872\,q^5-67284\,q^4 \\
&\quad +95081\,q^3-55748\,q^2-56196\,q+35280\Big)q \\
A_9(q) &= -4(q-2)\Big(126\,q^{19}-1155\,q^{18}+2898\,q^{17}+4734\,q^{16}-45150\,q^{15}+108141\,q^{14}-60851\,q^{13} \\
&\quad -251137\,q^{12}+637627\,q^{11}-612699\,q^{10}+26580\,q^9+675483\,q^8-807465\,q^7+293991\,q^6+84801\,q^5 \\
&\quad -74122\,q^4+66898\,q^3-85276\,q^2-49104\,q+40320\Big)q \\
A_{10}(q) &= \big(42\,q^{24}-630\,q^{23}+3060\,q^{22}+7065\,q^{21}-148760\,q^{20}+667161\,q^{19}-971176\,q^{18}-2513430\,q^{17} \\
&\quad +14478573\,q^{16}-28181285\,q^{15}+14657832\,q^{14}+51350346\,q^{13}-133352087\,q^{12}+139182213\,q^{11} \\
&\quad -33173604\,q^{10}-102090456\,q^9+154331241\,q^8-96138111\,q^7+10416711\,q^6+17983764\,q^5 \\
&\quad -9578403\,q^4+8318628\,q^3-4658148\,q^2-5973264\,q+3265920\big)q-\tau(q)q^{19}.
\end{aligned}
$$

We will combine this computation with the expansion of $W^s_{C'_{2,4}}(X+(q-1)Y, X-Y)$ given later in this chapter.

We point out that the weight enumerator $W^{G1}_{C'_{2,4}}(X,Y)$, and equivalently, the weight enumerator $\mathrm{QR}_{C_{1,4}}(X, X^2, 1)$, can be understood in terms of the weight enumerator of a certain code from evaluation of homogeneous quartics in a weighted projective space. Let $\mathbb{P}(2,1,1)$ denote the weighted projective space with coordinates

$[w : x : y]$ where w has weight 2 and x, y each has weight 1. Now consider the q^5 homogeneous quartics given by $w^2 = f_4(x, y)$ with $f_4(x, y)$ a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$. We take such a quartic to a codeword by evaluating at the $q^2 + q$ nonsingular points of $\mathbb{P}(2, 1, 1)$. These q^5 codewords do not form a linear code since we have fixed the coefficient of w to be 1. However, we see that the information given by the weight enumerator of this nonlinear code of size q^5 is exactly equivalent to the information given by $\mathrm{QR}_{C_{1,4}}(X, X^2, 1)$.

Theorem 52 implies the following.

Proposition 54. *Consider the weight enumerator $W_{C'_{1,4}}(X, Y)$ of the nonlinear code of size q^5 given by evaluating homogeneous quartics $w^2 = f_4(x, y)$ on $\mathbb{P}(2, 1, 1)$. Then*

$$W_{C'}(X + (q-1)Y, X - Y) = q^5 X^{q^2+q} + \sum_{j=1}^{10} A_j(q) X^{q^2+q-i} Y^j,$$

where $A_j(q)$ is a polynomial for $j \in [1, 9]$, and $A_{10}(q)$ is a polynomial in q plus $\tau(q)$ times a polynomial in q.

We will use this result in the last section of Chapter 4 when we consider certain configurations of low-weight dual codewords for codes coming from homogeneous quartics on $\mathbb{P}(2, 1, 1, 1)$.

We now return to the quadratic residue weight enumerator of $C_{1,4}$. We begin with the case where $q \equiv 1 \pmod 4$. Computation suggests that the dual code coefficients of weight 6 break up as follows:

$$\begin{aligned} \mathrm{QR}_{C_{1,4}^\perp}(X, Y, Z) &= X^{q+1} + (q-1)^2 q(q+1) X^{q-5} \Bigg(\frac{(q-3)(q^2-6q+53)}{23040} (Y^6 + Z^6) \\ &+ \frac{(q-5)(q-3)(q-1)}{1536} (Y^4 Z^2 + Y^2 Z^4) \Bigg), \end{aligned}$$

plus terms of the form $X^{q+1-(i+j)} Y^i Z^j$ where $i + j \geq 7$. As a check, we see that setting $Y = Z$ does give the Y^6 coefficient of the Hamming weight enumerator of

$C_{1,4}^{\perp}$. The case $q \equiv 3 \pmod 4$ is similar:

$$\begin{aligned}\mathrm{QR}_{C_{1,4}^{\perp}}(X,Y,Z) &= X^{q+1} + (q-1)^2 q(q+1) X^{q-5} \\ &\times \left(\frac{(q-3)(q-1)^2 q(q+1)(q^2-6q+17)}{1152} Y^3 Z^3 \right. \\ &+ \left. \frac{(q-7)(q-3)(q-1)^3 q(q+1)^2}{3840} (Y^5 Z + Y Z^5) \right),\end{aligned}$$

except that the product of the nonzero coordinates of a weight 6 codewords is a non-square in $\mathbb{F}_q^*$. We use this fact in Chapter 4.

Interestingly, the coefficients of weight 7 for all $q \geq 5$ with the characteristic of $\mathbb{F}_q$ odd are not given by polynomials in q. If the $X^{q-6}Y^7$ coefficient, for example, were given by a polynomial then the argument above shows that its degree would be at most 28. Computing with all small primes congruent to 1 modulo 4 shows that no polynomial fits all of these coefficients. We have also computed that this coefficient is not given by $P_1(q) + P_2(q)f(q)$ where $P_1(q)$ and $P_2(q)$ are polynomials of degree at most 26 and $f(q)$ is either $\tau(q)$, or the coefficient of the $e^{2\pi i z q}$ term of the Fourier series expansion of the unique cusp form of weight 8 on $\Gamma_0(2)$. In future work, we would like to determine what inputs determine these counts.

We now return to the proof of Theorem 52. This is related to earlier work of Birch in which he considers powers of traces of elliptic curves over finite fields [**3**]. Let Γ be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Let $N_p(\Gamma)$ denote the number of points of Γ_p, the reduction of Γ modulo p. Hasse's theorem shows that $N_p(\Gamma) = p + 1 - E_p(\Gamma)$, where $E_p(\Gamma) = 2\sqrt{p}\cos(\theta_p(\Gamma))$, where $0 \leq \theta_p(\Gamma) \leq \pi$. For a fixed curve Γ the distribution of these angles $\theta_p(\Gamma)$ is the subject of the famous Sato-Tate conjecture, now a theorem of Clozel, Harris, Shepherd-Barron, and Taylor [**10**]. We are interested only in the far easier case where the field $\mathbb{F}_q$ is fixed and the curve E is allowed to vary. The distribution of angles on these curves also satisfy a

kind of Sato-Tate distribution that is proven in the following form by Birch [**3**]. He focuses only on $\mathbb{F}_p$, but the behavior when $q = p^f$ for $f > 1$ should be similar.

Given an equation of a curve E in Weierstrass form $y^2 = x^3 - ax - b$, the trace of E, $p + 1$ minus the number of $\mathbb{F}_p$-rational points, is given by

$$p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 - ax - b}{p} \right).$$

This formula holds for elliptic curves as well as for singular curves. Let

$$S_R(p) = \sum_{a,b=0}^{p-1} \left(\sum_{x=0}^{p-1} \left(\frac{x^3 - ax - b}{p} \right) \right)^{2R}.$$

Birch computes that the average over pairs (a, b) of the $2R$ power of the trace of the curve in Weierstrass form $y^2 = x^3 - ax - b$ is given by $p^{-2} S_R(p) + O(p^{R-1})$. We gain information about average values of powers of point counts by studying $S_R(p)$.

Theorem 55 (Birch)**.** *We have*

$$S_R(p) \sim \frac{2R!}{R!(R+1)!} p^{R+2}, \quad \text{as } R \to \infty.$$

These moments match those of the Sato-Tate distribution. Birch also gives exact formulas for $R \leq 5$, polynomials in p for $R \in [1, 4]$ and a polynomial in p minus $\tau(p)$ for $R = 5$. In order to get these exact formulas he rewrites $S_R(p)$ in terms of a sum of Kronecker class numbers. This sum of Kronecker class numbers can be expressed in terms of $\sigma_k(T_p)$, the trace of the Hecke operator T_p acting on the space of cusp forms of weight $2 + 2k$ on $\mathrm{SL}_2(\mathbb{Z})$. The same strategy applied to dual code coefficients of weight $2k$ will prove Theorem 52.

Unfortunately, there is a well-known typo in this paper, so the exact formulas are off by a small factor [**37**]. The proof of this result uses a version of the Selberg trace formula, which we will not discuss here.

The connection between powers of traces of elliptic curves and the weight enumerator $W_C^{G1}(X+(q-1)Y, X-Y)$ should be clear. Each homogeneous quartic $f_4(x,y)$ such that $w^2 = f_4(x,y)$ defines an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q+1-t$ contributes a monomial to this weight enumerator, $X^{q^2+q-tq+1}Y^{q^3+tq-1}$. Substituting $X+(q-1)Y$ for X and $X-Y$ for Y shows that this term contributes

$$(X+(q-1)Y)^{q^2+q-tq+1}(X-Y)^{q^3+tq-1} \pmod{Y^{11}}$$

to the first 10 dual code coefficients. The Y^j term of this expansion can be expressed in terms of the first j powers of t. Taking the sum over all such quartics shows how the dual code coefficients are related to these powers of traces.

Consider the sum

$$S'_R(q) := \sum_{E/\sim} t^{2k},$$

where $E/\sim$ denotes the sum over all isomorphism classes of elliptic curves E over $\mathbb{F}_q$ where $\#E(\mathbb{F}_q) = q+1-t$, and the isomorphism classes are counted in inverse proportion to the size of $\mathrm{Aut}(E)$.

The exact counts in [**3**] use the fact that this sum can be expressed as a linear combination of the trace of the Hecke operator T_p acting on the full space of cusp forms of weight $2+2k$ for $\mathrm{SL}_2(\mathbb{Z})$ where the coefficients are polynomials in p. This is exactly the fact needed to prove Theorem 52 for fields of prime order.

We point out that this result of Birch is written only for fields of prime order. For $q = p^k$ with $k > 1$ we should technically replace the statement that $A_{10}(q)$ is a polynomial in q plus a polynomial in q times $\tau(q)$ with the statement that $A_{10}(q)$ is a polynomial in q plus a polynomial in q times $S'_R(q)$. In future work we plan to analyze this sum in the prime power case to address this issue.

We will use Proposition 53 in Chapter 4 as part of the proof of Theorem 3. The contribution of the this non-elementary term involving 10th powers of traces of elliptic

curves will exactly cancel with the computation of a certain dual code coefficient. Therefore, this prime power issue is not relevant to the proof of Theorem 3.

8. Quartic Curves with Non-Isolated Singularities

Our main goal is to find the distribution of point counts as we vary through the q^{15} varieties in $\mathbb{P}(2,1,1,1)$ given by $w^2 = f_4(x,y,z)$, where $f_4(x,y,z)$ is a homogeneous plane quartic. The discussion of the previous sections gives us a way to understand the contribution to this weight enumerator from cones over genus one curves given by $w^2 = f_4(x,y)$, for example, the contribution coming from quartics $f_4(x,y,z)$ where $f_4(x,y,z)$ is actually homogeneous in x and y and has no repeated root. This lets us compute the weight enumerator $W^{G1}_{C'_{2,4}}(X,Y)$ and its contribution to dual codewords of weight up to 10, $W^{G1}_{C}(X+(q-1)Y, X-Y)$ modulo Y^{11}.

We need to understand the contribution to the weight enumerator coming from quartics $f_4(x,y,z)$ with non-isolated singularities. We first observe that a cone over a variety $w^2 = f_4(x,y)$ where $f_4(x,y)$ is singular has a non-isolated singularity. We know that $f_4(x,y)$ is singular if and only if it has a double root. If $f_4(x,y)$ has a root of multiplicity at least two, the cone contains a line with the same multiplicity. Therefore, when we consider the contribution to the weight enumerator coming from varieties of the form $w^2 = f_4(x,y)$, we want to also assume that $f_4(x,y)$ is nonsingular, that this equation gives a genus 1 curve.

We recall that the contribution to this weight enumerator coming from varieties given by $w^2 = f_4(x,y,z)$ where $f_4(x,y,z)$ has non-isolated singularities is called $W^{s}_{C'_{2,4}}(X,Y)$. We actually give more information, computing the contribution to the quadratic residue weight enumerator coming from these terms.

This weight enumerator can be divided into two parts. There are quartics with a double component that do not vanish to degree 2 on a line, and those that do. Let $\mathrm{QR}^{snL}_{C'_{2,4}}(X,Y,Z)$ be the contribution from quartics of this first type, and $\mathrm{QR}^{sL}_{C'_{2,4}}(X,Y,Z)$

be the contribution from quartics of the second type. The terms 'sL' and 'snL' reflect whether the variety contains a double $\mathbb{F}_q$-rational line.

Lemma 56. *We have*

$$\mathrm{QR}^{snL}_{C'_{2,4}}(X,Y,Z) = \frac{q-1}{2}(q^5-q^2)X^{q+1}(Y^{q^2}+Z^{q^2}) + \frac{q-1}{2}\frac{q^4-q}{2}X(Y^{q^2+q}+Z^{q^2+q}).$$

Proof. The only types of quartics that contribute to this sum are double smooth conics and the union of two Galois-conjugate double lines defined over $\mathbb{F}_{q^2}$.

The contribution from the double smooth conics is

$$\frac{q-1}{2}(q^5-q^2)X^{q+1}(Y^{q^2}+Z^{q^2}),$$

since there are q^5-q^2 smooth conics, such a quartic $f(x,y,z)^2$ takes only square nonzero values, and the number of squares in $\mathbb{F}_q^*$ is equal to the number of non-squares, $\frac{q-1}{2}$.

The contribution from double Galois-conjugate $\mathbb{F}_{q^2}$-rational lines is

$$\frac{q-1}{2}\frac{q^4-q}{2}X(Y^{q^2+q}+Z^{q^2+q}),$$

since there are $\frac{q^4-q}{2}$ such conjugate lines, and $f(x,y,z)^2$ takes only square nonzero values, and we have $\frac{q-1}{2}$ choices of a scalar multiple. □

We also single out the contribution from one other type of quartic. The contribution from the union of two $\mathbb{F}_q$-rational double lines is

$$\frac{q-1}{2}\frac{(q^2+q+1)(q^2+q)}{2}X^{2q+1}(Y^{q^2-q}+Z^{q^2-q}).$$

We isolate this term because every other quartic with a non-isolated singularity contains a unique line with multiplicity two or greater. All lines are equivalent under automorphisms of $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, we will determine the weight enumerator coming from a particular choice of a fixed double line and the product with each of the

q^6-1 nonzero conics. There is a slight double counting issue since the product of two $\mathbb{F}_q$-rational double lines will be counted twice. Therefore, we count the contribution of all such pairs of double lines and subtract half of it.

Lemma 57. *We have*

$$\begin{aligned}\mathrm{QR}^{sL}_{C'_{2,4}}(X,Y,Z) &= (q^2+q+1)\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z)\\ &- \frac{1}{2}\frac{q-1}{2}\frac{(q^2+q+1)(q^2+q)}{2}X^{2q+1}(Y^{q^2-q}+Z^{q^2-q}),\end{aligned}$$

where $\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z)$ *is the contribution coming from the product of the double line* $x^2=0$ *and the* q^6-1 *nonzero conics in* $\mathbb{P}^2(\mathbb{F}_q)$.

Lemma 58. *We have*

$$\begin{aligned}\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z) &= \frac{(q-1)}{2}X^{q+1}(Y^{q^2}+Z^{q^2})\\ &+ \frac{q-1}{2}(q^2+q)X^{2q+1}(Y^{q^2-q}+Z^{q^2-q})\\ &+ (q-1)q^2\frac{q(q-1)}{2}X^{q+2}Y^{\frac{q^2-1}{2}}Z^{\frac{q^2-1}{2}}\\ &+ \frac{q-1}{2}(q+1)\frac{q(q-1)}{2}X^{q+1}(Y^{\frac{q^2-q}{2}}Z^{\frac{q^2+q}{2}}+Y^{\frac{q^2+q}{2}}Z^{\frac{q^2-q}{2}})\\ &+ (q-1)\frac{q^2(q^2+q)}{2}X^{3q}Y^{\frac{q^2-2q+1}{2}}Z^{\frac{q^2-2q+1}{2}}\\ &+ \frac{q-1}{2}\frac{q(q-1)}{2}(q+1)X^{3q+1}(Y^{\frac{q^2-3q}{2}}Z^{\frac{q^2-q}{2}}+Y^{\frac{q^2-q}{2}}Z^{\frac{q^2-3q}{2}})\\ &+ (q-1)(q+1)(q^3-q^2+q)X^{2q+1}Y^{\frac{q^2-q}{2}}Z^{\frac{q^2-q}{2}}\\ &+ \frac{q-1}{2}\frac{q^2-q}{2}(q^3-q^2)X^{2q+2}(Y^{\frac{q^2-2q-1}{2}}Z^{\frac{q^2-1}{2}}+Y^{\frac{q^2-1}{2}}Z^{\frac{q^2-2q-1}{2}})\\ &+ \frac{q-1}{2}\frac{q(q+1)}{2}(q^3-q^2)X^{2q}(Y^{\frac{q^2+1}{2}}Z^{\frac{q^2-2q+1}{2}}+Y^{\frac{q^2-2q+1}{2}}Z^{\frac{q^2+1}{2}}).\end{aligned}$$

Proof. The general idea is that $w^2=f_2(x,y,z)$ where $f_2(x,y,z)$ defines a conic in $\mathbb{P}^2(\mathbb{F}_q)$ gives the equation of a quadric in $\mathbb{P}^3(\mathbb{F}_q)$. We consider each type of $f_2(x,y,z)$ that arises up to projective isomorphism. We can choose some representative equation

for such a quartic and determine the number of points on the corresponding quadric in $\mathbb{P}^3(\mathbb{F}_q)$. We consider the quartic $f_4(x,y,z)$ that is $f_2(x,y,z)$ times the square of our chosen linear form and determine how many of the coordinates of the corresponding codeword are nonzero squares and how many are non-squares. Suppose that this linear form defines a line L in $\mathbb{P}^2(\mathbb{F}_q)$. We then consider the restriction of $f_2(x,y,z)$ to L. Combining our knowledge of the quadric in $\mathbb{P}^3(\mathbb{F}_q)$ given by $w^2 = f_2(x,y,z)$ with our knowledge of the $f_2(x,y,z)$ restricted to L lets us determine the contribution to the weight enumerator from the quartic $f_4(x,y,z)$. Since this restriction of $f_2(x,y,z)$ to L gives a quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_q)$, there are not too many cases to consider.

We explain each term that appears in the statement of this lemma in order. We first consider double lines. We choose the square of the linear form defining L. This vanishes at all $q+1$ points and takes square values at the other q^2 points of $\mathbb{P}^2(\mathbb{F}_q)$. Multiplying by a non-square gives an equation that vanishes at exactly $q+1$ points and otherwise takes non-square values. Now we consider a polynomial defining the union of two distinct $\mathbb{F}_q$-rational lines. Such a variety has $2q+1-\mathbb{F}_q$ rational points. The square of such a polynomial takes nonzero values that are all squares or all non-squares depending on which nonzero scalar we choose. There are q^2+q lines distinct from L.

For the next term, we consider a polynomial defining the product of two Galois-conjugate lines with their $\mathbb{F}_q$-rational point of intersection not lying on L. This gives $q+2$ total $\mathbb{F}_q$-rational points. There are $\frac{q^4-q}{2}$ pairs of Galois-conjugate lines and $\frac{q^4-q}{2}\frac{q^2}{q^2+q+1} = \frac{q^4-q^3}{2}$ of them intersect off our given line. This implies that $\frac{q^3-q}{2}$ of them do intersect on L. This polynomial restricts to a quadric with two Galois-conjugate roots on L. The contribution from the $q+1$ points of L is $Y^{\frac{q+1}{2}}Z^{\frac{q+1}{2}}$. The quadric in $\mathbb{P}^3(\mathbb{F}_q)$ coming from a pair of Galois-conjugate lines is a quadric cone, which has q^2+q+1 $\mathbb{F}_q$-rational points. Therefore, since we have $q+2$ rational zeros, there must be $\frac{q^2+q+1-(q+2)}{2} = \frac{q^2-1}{2}$ nonzero square values taken by this polynomial. This

means that there are just as many nonzero non-square values. This completes the explanation for this term.

For the next term, corresponding to the $\frac{q^3-q^2}{2}$ pairs of Galois-conjugate lines with their point of intersection on L, we note that there are now only $q+1$ $\mathbb{F}_q$-points, and that this polynomials restricted to L has a double root. The contribution of such a polynomial restricted to L is either XY^q or XZ^q depending on the restriction of this conic to L, whether it is a square in $\mathbb{F}_q^*$ times a square, or a non-square in $\mathbb{F}_q^*$ times a square. Each of these possibilities arises equally often. The resulting quadric in $\mathbb{P}^3(\mathbb{F}_q)$ is a cone with q^2+q+1 points, so there are either $\frac{q^2-((2q+1)-(q+1))}{2} = \frac{q^2-q}{2}$ coordinates that are squares, or $\frac{q^2-(1-(q+1))}{2} = \frac{q^2+q}{2}$ such coordinates.

The next term corresponds to the union of two distinct $\mathbb{F}_q$-rational lines. We consider two cases based on whether or not the point of intersection of these two lines lies on L. First suppose that it does not. There are q^2 choices for the point of intersection and $\frac{(q+1)q}{2}$ pairs of distinct $\mathbb{F}_q$-rational lines intersecting at that point. This polynomial restricted to L has two $\mathbb{F}_q$-rational zeros, so the contribution to the quadratic residue weight enumerator from the points of L is $X^2Y^{\frac{q-1}{2}}Z^{\frac{q-1}{2}}$. The quadric in $\mathbb{P}^3(\mathbb{F}_q)$ coming from this union of lines is a cone. Therefore there must be $\frac{q^2+q+1-3q}{2} = \frac{q^2-2q+1}{2}$ nonzero coordinates that are squares and the same number of non-squares.

Now, if the intersection of our two $\mathbb{F}_q$-rational lines lies on L, this quartic has $3q+1$ rational points. The polynomial defining this union of lines restricts to a polynomial with a double root on L, which contributes either XY^q or XZ^q to our weight enumerator depending on which scalar multiple we take. The resulting quadric in $\mathbb{P}^3(\mathbb{F}_q)$ is a cone. There are either $\frac{q^2+q+1-(3q+1)-(1-(q+1))}{2} = \frac{q^2-q}{2}$ coordinates that are nonzero squares, or $\frac{q^2+q+1-(3q+1)-(2q+1-(q+1)}{2} = \frac{q^2-3q}{2}$ coordinates that are nonzero squares. Each of these possibilities occurs equally often.

The next term breaks down into two pieces. We first consider when the polynomial gives a union of two $\mathbb{F}_q$-rational lines, exactly one equal to L. There are $q(q+1)$ such pairs of lines. This polynomial is identically 0 when restricted to L and the quadric in $\mathbb{P}^3(\mathbb{F}_q)$ resulting from it is again a cone. There are $\frac{q^2+q+1-(2q+1)}{2} = \frac{q^2-q}{2}$ coordinates that are squares, so there is the same number of non-squares.

Finally, we consider smooth conics intersecting L. We point out that the variety $w^2 = f_2(x,y,z)$ where $f_2(x,y,z)$ defines a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$ is a smooth quadric in $\mathbb{P}^3(\mathbb{F}_q)$. So, it is either a plus quadric, isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ with $(q+1)^2$ rational points, or a minus quadric with q^2+1 points.

First we consider conics that are tangent to the line L at some point. There are $(q^5-q^2)(q+1)$ pairs of a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$ along with a $\mathbb{F}_q$-rational line tangent to it at a point. Dividing by the number of lines and then again by the number of points on L, there are $q^2(q-1)$ smooth conics tangent to L at a given point. We note that each point of $\mathbb{P}^2(\mathbb{F}_q)$ not on L lies on a unique line through the point of tangency and another $\mathbb{F}_q$-rational point on the conic. We see that the contribution to the quadratic residue weight enumerator of the conic on any such line is $X^2 Y^{\frac{q-1}{2}} Z^{\frac{q-1}{2}}$, since it must restrict to a polynomial on this line with two distinct $\mathbb{F}_q$-points. Summing over the q lines shows that a conic tangent to a point of L contributes $X^{2q+1} Y^{\frac{q(q-1)}{2}} Z^{\frac{q(q-1)}{2}}$.

We next consider smooth conics that intersect L at two Galois-conjugate points. There are $\frac{q^2-q}{2}$ such pairs of points on L, and $\frac{q^4-q}{2}$ total such pairs of points. Each smooth conic passes through $q+1$ $\mathbb{F}_q$-rational points and q^2+1 $\mathbb{F}_{q^2}$-rational points, so it must pass through $\frac{q^2-q}{2}$ pairs of Galois-conjugate $\mathbb{F}_{q^2}$-points. Therefore we have $(q^5-q^2)(\frac{q^2-q}{2})$ pairs of a smooth conic and a pair of conjugate points on it. Dividing by $\frac{q^4-q}{2}$, we see that there are $q^2(q-1)$ smooth conics through a given pair of conjugate points.

The restriction to L of the polynomial defining a smooth conic passing through two conjugate points on L gives $\frac{q+1}{2}$ nonzero squares and the same number of non-squares. We choose any rational point of this conic and consider all of the lines passing through it. Every point in $\mathbb{P}^2(\mathbb{F}_q)$ aside from this chosen point is on a unique such line. We see that q of these lines pass through another $\mathbb{F}_q$-point of the conic, but the tangent line does not. Each of these q lines contributes $X^2Y^{\frac{q-1}{2}}X^{\frac{q-1}{2}}$ to the quadratic residue weight enumerator. The tangent line contributes either XY^q or XZ^q, each possibility occurring equally often as we vary over the $q-1$ scalar multiples of the conic. We must adjust the quadratic residue weight enumerator to account for the restriction of the conic to L. Instead of the term $Y^{\frac{q+1}{2}}Z^{\frac{q+1}{2}}$ coming from the conic restricted to L, we have X^{q+1} from L. Therefore, this quartic contributes

$$X^{2q+2}Y^{q\frac{q-1}{2}-\frac{q+1}{2}+q}Z^{q\frac{q-1}{2}-\frac{q+1}{2}},$$

to the quadratic residue weight enumerator if the polynomial defining the conic restricts to a square in $\mathbb{F}_q^*$ times a square on the line tangent to the chosen $\mathbb{F}_q$-point, and the same term but with Y and Z switched otherwise.

Finally, we consider smooth conics passing through two distinct rational points of L. There are $\frac{(q^2+q+1)(q^2+q)}{2}$ pairs of distinct $\mathbb{F}_q$-points, $\frac{(q+1)q}{2}$ of which lie on L. Each smooth conic passes through $\frac{(q+1)q}{2}$ pairs of $\mathbb{F}_q$-points. Therefore, there are

$$\frac{(q^5-q^2)\frac{(q+1)q}{2}}{\frac{(q^2+q+1)(q^2+q)}{2}} = (q^3-q^2),$$

smooth conics through each pair of $\mathbb{F}_q$-points.

We choose one of the two $\mathbb{F}_q$-rational points in the intersection of the conic and L, and consider all the lines through it. There are q lines on which the contribution of the conic restricted to L is $X^2Y^{\frac{q-1}{2}}Z^{\frac{q-1}{2}}$, including L. The last of these lines is tangent to the conic and on this line it either restricts to XY^q or XZ^q with each possibility occurring equally often. Therefore, the contribution of such quartics to

the quadratic residue weight enumerator is

$$\frac{q-1}{2}\frac{q(q+1)}{2}(q^3-q^2)X^{2q}(Y^{q\frac{q-1}{2}-\frac{q-1}{2}+q}Z^{q\frac{q-1}{2}-\frac{q-1}{2}}+Y^{q\frac{q-1}{2}-\frac{q-1}{2}}Z^{q\frac{q-1}{2}-\frac{q-1}{2}+q}).$$

This completes the proof. □

Alternatively, we could have given a proof in the following way. We could argue from the form of the terms contributing to $\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z)$ that all of its coefficients will be polynomials in q. By computing $\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z)$ for the first several primes, say the first 10 odd primes or so, and arguing that the degree of each polynomial will be at most 6, we can find the coefficient of each term of $\mathrm{QR}^{DL}_{C'_{2,4}}(X,Y,Z)$ by polynomial interpolation. In the next chapter we will need to solve a similar problem where the case-by-case analysis is too intricate.

We next turn to the contribution of $W^s_{C'_{2,4}}(X,Y)$ to the low-weight codewords of $C'^{\perp}_{2,4}$. We could apply the MacWilliams identity for quadratic residue weight enumerators to gain information about how the coordinates of low-weight dual codewords split up into nonzero squares and non-squares, however this is more information than we need. We instead consider

$$\mathrm{QR}^{snL}_{C'_{2,4}}(X,X^2,1)+\mathrm{QR}^{sL}_{C'_{2,4}}(X,X^2,1),$$

homogenized to a polynomial of degree q^3+q^2+q in X and Y. This degree is the number of points in the weighted projective space $\mathbb{P}(2,1,1,1)$ omitting the singular point. This homogenized polynomial is the $W^s_{C'_{2,4}}(X,Y)$ defined in Chapter 2. Since the coefficients of this weight enumerator are polynomials in q, applying the linear transformation form the MacWilliams identity produces contributions to dual code coefficients that are also polynomial in q.

Theorem 59. *$W^s_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11} is equal to*

$$(q^3-1)\sum_{j=0}^{10}\frac{A_j(q)}{j!}X^{q^3+q^2+q-j}Y^j + O(Y^{11}),$$

where the values of $A_j(q)$ are:

$$\begin{aligned}
A_0(q) &= q^5+q^4+2\,q^3+1, \quad A_1(q)=0, \quad A_2(q)=\big(q^8-2\,q^7-q^6+q^5+q^3+1\big)q\\
A_3(q) &= -(q-2)\big(4\,q^8-5\,q^7-q^6+2\,q^5-q^4+2\,q^3+2\big)q\\
A_4(q) &= \big(q^{14}-8\,q^{12}+11\,q^{11}+17\,q^{10}-68\,q^9+100\,q^8-51\,q^7-20\,q^6+39\,q^5-36\,q^4+18\,q^3+6\,q^2-15\,q+18\big)q\\
A_5(q) &= -2(q-2)\Big(5\,q^{14}-35\,q^{12}+45\,q^{11}+38\,q^{10}-118\,q^9+156\,q^8-89\,q^7-15\,q^6+57\,q^5-60\,q^4+24\,q^3\\
&\quad +12\,q^2-14\,q+24\Big)q\\
A_6(q) &= \Big(q^{20}-15\,q^{18}+10\,q^{17}+146\,q^{16}-381\,q^{15}-234\,q^{14}+2445\,q^{13}-3638\,q^{12}-109\,q^{11}+6239\,q^{10}-8730\,q^9\\
&\quad +6916\,q^8-2040\,q^7-2040\,q^6+3325\,q^5-2280\,q^4+130\,q^3+785\,q^2-770\,q+600\Big)q\\
A_7(q) &= -(q-2)\Big(21\,q^{20}-280\,q^{18}+210\,q^{17}+1736\,q^{16}-3451\,q^{15}-2093\,q^{14}+15561\,q^{13}-21293\,q^{12}\\
&\quad +1859\,q^{11}+28299\,q^{10}-36317\,q^9+27195\,q^8-8294\,q^7-7047\,q^6+12120\,q^5-9000\,q^4+204\,q^3\\
&\quad +2982\,q^2-2052\,q+2160\Big)q\\
A_8(q) &= \Big(q^{26}-28\,q^{24}+21\,q^{23}+532\,q^{22}-1414\,q^{21}-3296\,q^{20}+18024\,q^{19}-6236\,q^{18}-90587\,q^{17}\\
&\quad +169532\,q^{16}+60557\,q^{15}-609723\,q^{14}+917659\,q^{13}-414191\,q^{12}-677404\,q^{11}+1373296\,q^{10}-1181278\,q^9\\
&\quad +575351\,q^8+30205\,q^7-346262\,q^6+344036\,q^5-143948\,q^4-59143\,q^3+85372\,q^2-56196\,q+35280\Big)q\\
A_9(q) &= -4(q-2)\Big(9\,q^{26}-231\,q^{24}+189\,q^{23}+2709\,q^{22}-5481\,q^{21}-12990\,q^{20}+54612\,q^{19}-17036\,q^{18}\\
&\quad -209160\,q^{17}+365393\,q^{16}+106430\,q^{15}-1070395\,q^{14}+1460443\,q^{13}-616234\,q^{12}-921947\,q^{11}\\
&\quad +1837128\,q^{10}-1466383\,q^9+655377\,q^8+59587\,q^7-394022\,q^6+371404\,q^5-167992\,q^4\\
&\quad -73430\,q^3+96164\,q^2-49104\,q+40320\Big)q\\
A_{10}(q) &= \Big(q^{32}-45\,q^{30}+36\,q^{29}+1500\,q^{28}-4050\,q^{27}-20700\,q^{26}+99498\,q^{25}+56509\,q^{24}-1001101\,q^{23}\\
&\quad +1206436\,q^{22}+4319196\,q^{21}-13616003\,q^{20}+4281177\,q^{19}+41588189\,q^{18}-76832522\,q^{17}+2845541\,q^{16}\\
&\quad +181091943\,q^{15}-298047467\,q^{14}+189503865\,q^{13}+78529809\,q^{12}-295879830\,q^{11}+313354185\,q^{10}\\
&\quad -176095173\,q^9+34145724\,q^8+47631213\,q^7-62669700\,q^6+38639664\,q^5-5261751\,q^4\\
&\quad -15015852\,q^3+11671452\,q^2-5973264\,q+3265920\Big)q.
\end{aligned}$$

We have now computed two of the key terms needed to understand $W^{DP}_{C'_{2,4}}(X,Y)$, the contribution from cones over genus 1 curves given by $w^2 = f_4(x,y)$, and from homogeneous quartics $w^2 = f_4(x,y,z)$ with non-isolated singularities. In the next chapter we will consider the contribution coming from the 15-dimensional subcode of cones over plane quartics, and the counts for dual codewords of weight up to 10. This dual code calculation will be the most intricate part of the proof of Theorem 3.

9. Other MacWilliams Theorems and Codes from Genus 1 Curves

Before moving on to the proof of Theorem 3 we return to variations of the MacWilliams theorem coming from character sums. We begin with cubic Gauss sums.

For $p \equiv 1 \pmod 3$, the prime p factors in $\mathbb{Z}[\omega]$ where ω is a primitive cube root of unity, as $\pi\overline{\pi} = p$ for some prime $\pi \in \mathbb{Z}[\omega]$. We have $\mathbb{F}_p^* / \left(\mathbb{F}_p^*\right)^3$ is a cyclic group of order three. There is a cubic character $\chi_\pi(\beta)$ taking values $1, \omega, \omega^2$ which determines the coset of β in this group. Let $\zeta_p = e^{2\pi i/p}$.

Proposition 60. *Let $p \equiv 1 \pmod 3$ be a prime and let ψ be an additive character on $\mathbb{F}_q$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of the polynomial $f(x) = x^3 - 3px - Ap$, where $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod 3$.*

Then

$$\sum_{x \in \mathbb{F}_p} \zeta_p^{x^3}$$

is one of the roots α_i. This is $3G_1 + 1$ where

$$G_1 = \sum_{x \ |\chi_\pi(x)=1} \psi(x).$$

The other two roots are $3G_2 + 1$ *and* $3G_3 + 1$ *where*

$$G_2 = \sum_{x \ | \chi_\pi(x) = \omega} \psi(x), \quad \textit{and } G_3 = \sum_{x \ | \chi_\pi(x) = \omega^2} \psi(x).$$

See Section 12 of Chapter 9 of [**27**] for a proof.

We can now state our cubic residue version of the MacWilliams Theorem. We will only state this for codes over prime fields.

Theorem 61. *Let* C *be a linear code of length* N *over* $\mathbb{F}_p$ *with* $p \equiv 1 \pmod 3$ *and let*

$$\mathrm{CR}_C(W, X, Y, Z) := \sum_{c \in C} \prod_{i=1}^{N} H(c_i),$$

where $c = (c_1, \ldots, c_N)$ *and*

$$H(x) = \begin{cases} W \ \textit{if } x = 0 \\ X \ \textit{if } \chi_\pi(x) = 1 \\ Y \ \textit{if } \chi_\pi(x) = \omega \\ Z \ \textit{if } \chi_\pi(x) = \omega^2 \end{cases}.$$

Then

$$\mathrm{CR}_C(W, X, Y, Y) = \frac{1}{|C^\perp|} \mathrm{CR}_{C^\perp}(W', X', Y', Y''),$$

where

$$W' = W + \frac{p-1}{3}(X + 2Y), \quad X' = W + G_1 X + (G_2 + G_3)Y,$$
$$Y' = W + G_2 X + (G_3 + G_1)Y, \quad Y'' = W + G_3 X + (G_1 + G_2)Y.$$

If $c = (c_1, \ldots, c_N) \in \mathbb{F}_q^N$ has α coordinates with $c_i = 0$, β coordinates with $\chi_\pi(c_i) = 1$, γ coordinates with $\chi_\pi(c_j) = \omega$, and δ coordinates with $\chi_\pi(c_i) = \omega^2$, then for some $\epsilon \in \mathbb{F}_q$ with $\chi_\pi(\epsilon) = \omega$ we see that $\epsilon c = (\epsilon c_1, \ldots, \epsilon c_N)$ has $(\alpha, \delta, \beta, \gamma)$ of each of these types of coordinates, and that $\epsilon^2 c$ has $(\alpha, \gamma, \delta, \beta)$ of each of these

coordinates. Since there are $\frac{p-1}{3}$ nonzero elements taking each possible value under χ_π and C is linear, we see that the linear transformation in this statement still holds if we replace (G_1, G_2, G_3) with (G_3, G_1, G_2) or (G_2, G_3, G_1). We note that it is not generally equivalent to the linear transformation where (G_1, G_2, G_3) is replaced by (G_2, G_1, G_3).

PROOF. We closely follow the strategy from the proof of the MacWilliams identity for the quadratic residue weight enumerator given at the beginning of this chapter. Let $\phi(c) = \prod_{i=1}^{N} H(c_i)$. So $\sum_{c \in C} \phi(c) = \mathrm{CR}_C(W, X, Y, Z)$. We see that the Fourier transform of ϕ is defined by

$$\hat{\phi}(\hat{g}) = \sum_{g \in \mathbb{F}_p^N} \psi(\langle g, \hat{g} \rangle) \phi(g).$$

Discrete Poisson summation gives

$$\sum_{c \in C} \phi(c) = \frac{1}{|C^\perp|} \sum_{d \in C^\perp} \hat{\phi}(d).$$

We consider the coordinates of $\hat{\phi}(d)$ one at a time. We have

$$\begin{aligned} \hat{\phi}(d) &= \sum_{g \in \mathbb{F}_p^N} \prod_{i=1}^{N} \psi(d_i g_i) H(g_i) = \prod_{i=1}^{N} \sum_{g_P \in \mathbb{F}_p} \psi(d_i g_i) H(g_i) \\ &= \prod_{i=1}^{N} \left(W + X \sum_{x \mid \chi_\pi(x)=1} \psi(x d_i) + Y \sum_{\substack{x \mid x \neq 0 \\ \chi_\pi(x) \neq 1}} \psi(x d_i) \right). \end{aligned}$$

We consider the internal sum. If $d_i = 0$, this is $W + \frac{p-1}{3}(X + 2Y)$. If $\chi_\pi(d_P) = 1$, this is

$$W + X \sum_{x \mid \chi_\pi(x)=1} \psi(x) + Y \sum_{\substack{x \mid x \neq 0 \\ \chi_\pi(x) \neq 1}} \psi(x) = W + G_1 X + (G_2 + G_3) Y.$$

If $\chi_\pi(d_i) = \omega$, this is

$$W + X \sum_{x \mid \chi_\pi(x)=\omega} \psi(x) + Y \sum_{\substack{x \mid x\neq 0 \\ \chi_\pi(x)\neq\omega}} \psi(x) = W + G_2X + (G_3 + G_1)Y.$$

Finally, if $\chi_\pi(d_i) = \omega^2$, this is

$$W + X \sum_{x \mid \chi_\pi(x)=\omega} \psi(x) + Y \sum_{\substack{x \mid x\neq 0 \\ \chi_\pi(x)\neq\omega}} \psi(x) = W + G_3X + (G_1 + G_2)Y.$$

Taking the product over all coordinates i and then the sum over all $d \in C^\perp$ completes the proof. □

We note that it is not strictly necessary to determine which of the three roots α_i of $x^3 - 3px - Ap$ satisfies $G_1 = \frac{\alpha_i - 1}{3}$. This is not easy to determine and is the subject of Kummer's conjecture for cubic Gauss sums, now a theorem of Heath-Brown [**25**]. We can simply choose some α_i, the largest one for example, and let $K_1 = \frac{\alpha_i - 1}{3}$. Then we substitute K_1 for G_1 and (K_2, K_3) for (G_2, G_3) where K_2 and K_3 and given in terms of the other two roots of the polynomial. One of these choices will lead to an identity that holds, and the others generally will not.

Just as we studied the quadratic residue weight enumerator for the code of homogeneous degree $2k$ forms on $\mathbb{P}^n(\mathbb{F}_q)$, we can study this cubic weight enumerator for homogeneous degree $3k$ forms on $\mathbb{P}^n(\mathbb{F}_q)$. In the simplest case, $k = 1,\ n = 1$, we get homogeneous cubics on $\mathbb{P}^1(\mathbb{F}_q)$. Like the quadratic residue weight enumerator applied to quartics on $\mathbb{P}^1(\mathbb{F}_q)$ led to the study of elliptic curves over finite fields, this setting also gives genus 1 curves, although a more restricted family.

Proposition 62. *Let $f_3(x, y)$ be a smooth homogeneous cubic on $\mathbb{P}^1(\mathbb{F}_p)$. Then $w^3 = f_3(x, y)$ is a genus 1 curve, an elliptic curve with j-invariant 0. Given an elliptic curve E defined over $\mathbb{F}_p$ with j-invariant 0 there is a homogeneous cubic $f_3(x, y)$ such that $w^3 = f_3(x, y)$ is isomorphic to E.*

PROOF. This is a standard fact about elliptic curves given as homogeneous cubics. For a general discussion of how to take such a cubic and put it into Weierstrass form see Section 1.4 of [**11**]. For a general definition of the j-invariant attached to a nonsingular homogeneous cubic, see the appendix of [**18**]. □

In future work we plan to compute $\mathrm{CR}_C(W, X, Y, Z)$ for this 4-dimensional code and study the low-weight coefficients of its dual. We can then study the code of diagonal cubic surfaces $w^3 = f_3(x, y, z)$ in $\mathbb{P}^3(\mathbb{F}_q)$. The weight enumerator of this code will contain a contribution from cones over these genus 1 curves of j-invariant 0. It would be interested to compare point counts for these diagonal cubics to point count for general cubic surfaces.

There is another natural setting for this type of variation of the MacWilliams identity. Using results on biquadratic Gauss sums we can prove a variation of this identity that keeps track of whether a coordinate is a 4th power or not modulo p. This weight enumerator can be applied to the code of quadrics on $\mathbb{P}^1(\mathbb{F}_q)$ leading to equations of the form $w^4 = f_2(x, y)$, where $f_2(x, y)$ is a quadric on $\mathbb{P}^1(\mathbb{F}_q)$ with distinct roots. Such an equation defines a genus 1 curve with j-invariant 1728. We can think of this as a homogeneous quartic in the weighted projective space $\mathbb{P}(1, 2, 2)$ where w has weight 1 and x and y each have weight 2. We plan to pursue this in future work.

CHAPTER 4

The Distribution of Point Counts for del Pezzo Surfaces of Degree 2

In this chapter we give the proof of Theorem 3. This will involve a computation of low-weight dual code coefficients for a particular 16-dimensional code, and for a related 15-dimensional code. We also use the geometry of $\mathbb{P}^2(\mathbb{F}_q)$ and facts about the Picard group of a del Pezzo surface of degree 2 to determine the number of equations $w^2 = f_4(x, y, z)$ with $q^2 + 8q + 1$ $\mathbb{F}_q$-points and with $q^2 + 7q + 1$ $\mathbb{F}_q$-points. We also describe interesting geometric consequences of Theorem 3 for small values of q.

1. A Sketch of the Proof

We recall the setup from Chapter 2. Let $C'_{2,4}$ be the 16-dimensional code coming from varieties of the form

$$\alpha w^2 = f_4(x, y, z),$$

which we can think of as homogeneous quartics in the weighted projective space $\mathbb{P}(2, 1, 1, 1)$. We also need to consider $C^c_{2,4}$, the 15-dimensional subcode from varieties with $\alpha = 0$.

We write

$$W_{C'_{2,4}}(X, Y) = W_{C^c_{2,4}}(X, Y) + (q - 1)W^D_{C'_{2,4}}(X, Y),$$

where $W^D_{C'_{2,4}}(X, Y)$ is the contribution to the weight enumerator from codewords with $\alpha = 1$. We let

$$W^D_{C'_{2,4}}(X, Y) = W^s_{C'_{2,4}}(X, Y) + W^{G1}_{C'_{2,4}}(X, Y) + W^{DP}_{C'_{2,4}}(X, Y),$$

where $W^s_{C'_{2,4}}(X,Y)$ is the contribution to this weight enumerator from equations of the form $w^2 = f_4(x,y,z)$ where $f_4(x,y,z)$ defines a plane quartic with non-isolated singularities, $W^{G1}_{C'_{2,4}}(X,Y)$ is the contribution to this weight enumerator from equations of the form $w^2 = f_4(x,y,z)$ where $f_4(x,y,z)$ gives the union of four coincident lines, a quartic curve with a non-simple elliptic singularity, and $W^{DP}_{C'_{2,4}}(X,Y)$ is the contribution to the weight enumerator from everything else. We have seen that

$$W^{DP}_{C'_{2,4}}(X,Y) = a_{-7}X^{q^2+q+1-(-7q)}Y^{q^3-7q-1} + \cdots + a_7 X^{q^2+q+1-(7q)}Y^{q^3+7q-1},$$

where $a_j = a_{-j}$ for $j \in [1,7]$.

In this chapter we find these 8 unknowns $a_0, a_1, \ldots, a_7$. A first major step will be determining the $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11}. It is clear that

$$\begin{aligned} W^{D}_{C'_{2,4}}(X+(q-1)Y, X-Y) &= W^{s}_{C'_{2,4}}(X+(q-1)Y, X-Y) \\ + \quad W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y) &+ W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y). \end{aligned}$$

The MacWilliams theorem implies that

$$q^{16}W_{C'^{\perp}_{2,4}}(X,Y) = W_{C^c_{2,4}}(X+(q-1)Y, X-Y) + (q-1)W^D_{C'_{2,4}}(X+(q-1)Y, X-Y),$$

and

$$W_{C^c_{2,4}}(X+(q-1)Y, X-Y) = q^{15}W_{C^{c\perp}_{2,4}}(X,Y).$$

In the previous chapter we computed

$$W^s_{C'_{2,4}}(X+(q-1)Y, X-Y) + W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y) \pmod{Y^{11}}.$$

Therefore, in order to compute $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11} we instead find $W_{C'^{\perp}_{2,4}}(X,Y)$ modulo Y^{11} and $W_{C^{c\perp}_{2,4}}(X,Y)$ modulo Y^{11}.

We first state our main results and postpone the proofs until later.

Theorem 63. *$W_{C_{2,4}^{c\perp}}(X,Y)$ modulo Y^{11} is equal to*

$$X^{q^3+q^2+q} + (q-1)^2 q(q^2+q+1) \sum_{j=2}^{10} \frac{A_j(q)}{j!} X^{q^3+q^2+q-j} Y^j + O(Y^{11}),$$

where the values of $A_j(q)$ are:

$$\begin{aligned}
A_2(q) &= 1, \quad A_3(q) = (q-2)^2 \\
A_4(q) &= (3\,q^5 - 2\,q^4 - 11\,q^3 + 27\,q^2 - 33\,q + 18) \\
A_5(q) &= (q-2)^2 (10\,q^5 - 9\,q^4 - 19\,q^3 + 38\,q^2 - 38\,q + 24) \\
A_6(q) &= (16\,q^{10} - 13\,q^9 - 237\,q^8 + 863\,q^7 - 1108\,q^6 - 274\,q^5 + 2790\,q^4 - 4180\,q^3 + 3525\,q^2 - 1970\,q + 600) \\
A_7(q) &= (q-2)\Big(q^{12} + 109\,q^{11} - 452\,q^{10} - 124\,q^9 + 3725\,q^8 - 8267\,q^7 + 6270\,q^6 + 5699\,q^5 - 18472\,q^4 \\
&\quad + 21651\,q^3 - 15312\,q^2 + 7452\,q - 2160\Big) \\
A_8(q) &= \Big(q^{16} + 135\,q^{15} - 138\,q^{14} - 4625\,q^{13} + 22564\,q^{12} - 32694\,q^{11} - 52554\,q^{10} + 287862\,q^9 - 490272\,q^8 \\
&\quad + 318928\,q^7 + 277242\,q^6 - 881251\,q^5 + 1056237\,q^4 - 807919\,q^3 + 430360\,q^2 - 162036\,q + 35280\Big) \\
A_9(q) &= (q-2)\Big(q^{18} + 40\,q^{17} + 1382\,q^{16} - 8928\,q^{15} + 491\,q^{14} + 129139\,q^{13} - 415145\,q^{12} + 358839\,q^{11} \\
&\quad + 953277\,q^{10} - 3280584\,q^9 + 4232208\,q^8 - 1611694\,q^7 - 3300122\,q^6 + 6798764\,q^5 - 6798260\,q^4 \\
&\quad + 4587408\,q^3 - 2201072\,q^2 + 760896\,q - 161280\Big) \\
A_{10}(q) &= \Big(q^{22} + 48\,q^{21} + 1734\,q^{20} - 5599\,q^{19} - 86758\,q^{18} + 641336\,q^{17} - 1337083\,q^{16} - 2292639\,q^{15} \\
&\quad + 18254124\,q^{14} - 39440054\,q^{13} + 21366100\,q^{12} + 84882388\,q^{11} - 239151303\,q^{10} + 290151336\,q^9 \\
&\quad - 123793500\,q^8 - 178740396\,q^7 + 406197288\,q^6 - 433630392\,q^5 + 312483609\,q^4 - 166440924\,q^3 \\
&\quad + 66046428\,q^2 - 19036944\,q + 3265920\Big).
\end{aligned}$$

Theorem 64. *$W_{C'^{\perp}_{2,4}}(X,Y)$ modulo Y^{11} is equal to*

$$X^{q^3+q^2+q} + (q-1)^2(q^2+q+1)\sum_{j=2}^{10} \frac{A_j(q)}{j!} X^{q^3+q^2+q-j}Y^j + O(Y^{11}),$$

where the values of $A_j(q)$ are:

$$\begin{aligned}
A_2(q) &= 1, \quad A_3(q) = (q-3)(q-2)\\
A_4(q) &= (3\,q^5 - 2\,q^4 - 11\,q^3 + 30\,q^2 - 48\,q + 36)\\
A_5(q) &= (q-2)\big(10\,q^6 - 29\,q^5 - q^4 + 76\,q^3 - 120\,q^2 + 142\,q - 120\big)\\
A_6(q) &= (16\,q^{10} - 13\,q^9 - 236\,q^8 + 854\,q^7 - 1073\,q^6 - 329\,q^5 + 2804\,q^4 - 4256\,q^3 + 4195\,q^2 - 3510\,q + 1800)\\
A_7(q) &= (q-2)\Big(q^{12} + 109\,q^{11} - 452\,q^{10} - 124\,q^9 + 3704\,q^8 - 8078\,q^7 + 5640\,q^6 + 6539\,q^5 - 18466\,q^4\\
&\quad +20892\,q^3 - 16467\,q^2 + 12582\,q - 7560\Big)\\
A_8(q) &= \Big(q^{16} + 135\,q^{15} - 138\,q^{14} - 4625\,q^{13} + 22565\,q^{12} - 32721\,q^{11} - 52050\,q^{10} + 283431\,q^9 - 470154\,q^8\\
&\quad +268885\,q^7 + 340997\,q^6 - 899977\,q^5 + 1005543\,q^4 - 770224\,q^3 + 510076\,q^2 - 330624\,q + 141120\Big)\\
A_9(q) &= (q-2)\Big(q^{18} + 40\,q^{17} + 1382\,q^{16} - 8928\,q^{15} + 491\,q^{14} + 129139\,q^{13} - 415265\,q^{12} + 360567\,q^{11}\\
&\quad +939809\,q^{10} - 3210332\,q^9 + 3988076\,q^8 - 1086638\,q^7 - 3894778\,q^6 + 6900916\,q^5 - 6222468\,q^4\\
&\quad +3976924\,q^3 - 2277288\,q^2 + 1448352\,q - 725760\Big)\\
A_{10}(q) &= \Big(q^{22} + 48\,q^{21} + 1734\,q^{20} - 5599\,q^{19} - 86758\,q^{18} + 641337\,q^{17} - 1336992\,q^{16} - 2294532\,q^{15}\\
&\quad +18273165\,q^{14} - 39568799\,q^{13} + 22020658\,q^{12} + 82256547\,q^{11} - 230767899\,q^{10} + 269456593\,q^9\\
&\quad -86914540\,q^8 - 219872635\,q^7 + 421463214\,q^6 - 404765268\,q^5 + 263019501\,q^4 - 138762972\,q^3\\
&\quad +74629836\,q^2 - 42930000\,q + 16329600\Big) - (q-1)(q+1)q^5\tau(q).
\end{aligned}$$

Combining these results with the computations of $W^{s}_{C'_{2,4}}(X+(q-1)Y, X-Y))$ and $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$, both modulo Y^{11}, gives the following statement.

Corollary 65. *$W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ modulo Y^{11} is given by*

$$A_0(q) + (q^3-1)(q^2-q)\sum_{j=2}^{10} \frac{A_j(q)}{j!} X^{q^3+q^2+q-j}Y^j + O(Y^{11}),$$

where the values of $A_j(q)$ are:

$$
\begin{aligned}
A_0(q) &= (q^{15} - q^8 - 2\,q^7 - 2\,q^6 + 2\,q^5 + 2\,q^4 + q^3 - q^2 + 1),\\
A_2(q) &= (-2\,q^8 + 3\,q^7 + 3\,q^6 - 2\,q^5 - 2\,q^4 - q^3 + q^2 - 1)\\
A_3(q) &= -(q-2)\big(q^{15} - 7\,q^8 + 7\,q^7 + 7\,q^6 - 4\,q^5 - 4\,q^4 - 2\,q^3 + 2\,q^2 - 2\big)\\
A_4(q) &= \Big(3\,q^{17} - 15\,q^{16} + 18\,q^{15} - q^{14} - 2\,q^{13} + 14\,q^{12} - 9\,q^{11} - 39\,q^{10} + 104\,q^9 - 121\,q^8 + 3\,q^7 + 87\,q^6 - 12\,q^5\\
&\quad -12\,q^4 - 33\,q^3 + 12\,q^2 + 15\,q - 18\Big)\\
A_5(q) &= -2(q-2)\Big(3\,q^{17} - 21\,q^{16} + 36\,q^{15} - 5\,q^{14} - 10\,q^{13} + 60\,q^{12} - 30\,q^{11} - 108\,q^{10} + 160\,q^9 - 150\,q^8 + 31\,q^7\\
&\quad +102\,q^6 - 32\,q^5 - 12\,q^4 - 38\,q^3 + 12\,q^2 + 14\,q - 24\Big)\\
A_6(q) &= \Big(q^{23} - 9\,q^{22} + 35\,q^{21} - 56\,q^{20} + 14\,q^{19} - 66\,q^{18} + 690\,q^{17} - 1717\,q^{16} + 1356\,q^{15} + 1246\,q^{14} - 3925\,q^{13}\\
&\quad +2918\,q^{12} + 4414\,q^{11} - 9606\,q^{10} + 7670\,q^9 - 4010\,q^8 - 770\,q^7 + 3260\,q^6 - 1315\,q^5 + 665\,q^4 - 900\,q^3\\
&\quad -185\,q^2 + 770\,q - 600\Big)\\
A_7(q) &= -(q-2)\Big(21\,q^{23} - 189\,q^{22} + 630\,q^{21} - 861\,q^{20} - 6\,q^{19} + 934\,q^{18} + 1505\,q^{17} - 7307\,q^{16} + 6296\,q^{15}\\
&\quad +9709\,q^{14} - 22953\,q^{13} + 14356\,q^{12} + 21954\,q^{11} - 41875\,q^{10} + 25181\,q^9 - 13479\,q^8 + 1938\,q^7 + 11352\,q^6\\
&\quad -7002\,q^5 + 2262\,q^4 - 2256\,q^3 - 822\,q^2 + 2052\,q - 2160\Big)\\
A_8(q) &= \Big(q^{27} - 28\,q^{26} + 504\,q^{25} - 4403\,q^{24} + 20083\,q^{23} - 50435\,q^{22} + 64791\,q^{21} - 16992\,q^{20} - 54354\,q^{19}\\
&\quad +5384\,q^{18} + 184751\,q^{17} - 187551\,q^{16} - 318878\,q^{15} + 897732\,q^{14} - 667990\,q^{13} - 408570\,q^{12} + 1350580\,q^{11}\\
&\quad -1213422\,q^{10} + 575302\,q^9 - 243789\,q^8 - 106414\,q^7 + 334726\,q^6 - 192759\,q^5 + 52920\,q^4 + 2947\,q^3\\
&\quad -50092\,q^2 + 56196\,q - 35280\Big)\\
A_9(q) &= -4(q-2)\Big(30\,q^{27} - 441\,q^{26} + 3367\,q^{25} - 17332\,q^{24} + 60718\,q^{23} - 132818\,q^{22} + 151373\,q^{21} - 18437\,q^{20}\\
&\quad -150512\,q^{19} + 66250\,q^{18} + 243915\,q^{17} - 177979\,q^{16} - 663788\,q^{15} + 1431957\,q^{14} - 849396\,q^{13} - 671948\,q^{12}\\
&\quad +1755992\,q^{11} - 1455636\,q^{10} + 574117\,q^9 - 287264\,q^8 - 41684\,q^7 + 405176\,q^6 - 255402\,q^5 + 42396\,q^4\\
&\quad +24326\,q^3 - 55844\,q^2 + 49104\,q - 40320\Big)\\
A_{10}(q) &= \Big(91\,q^{31} - 1848\,q^{30} + 19005\,q^{29} - 130287\,q^{28} + 659238\,q^{27} - 2608159\,q^{26} + 8276211\,q^{25}\\
&\quad -20599432\,q^{24} + 37219965\,q^{23} - 41516259\,q^{22} + 14127321\,q^{21} + 27031378\,q^{20} - 28077430\,q^{19}\\
&\quad -14089496\,q^{18} + 5884299\,q^{17} + 121271322\,q^{16} - 255860130\,q^{15} + 197868984\,q^{14} + 51768804\,q^{13}\\
&\quad -266034654\,q^{12} + 289927485\,q^{11} - 169439655\,q^{10} + 61973298\,q^9 - 14150610\,q^8 - 37966077\,q^7\\
&\quad +57749445\,q^6 - 24347772\,q^5 - 2662317\,q^4 + 9042588\,q^3 - 8405532\,q^2 + 5973264\,q - 3265920\Big)q.
\end{aligned}
$$

We are very fortunate that even though both $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ and $W_{C'^{\perp}_{2,4}}(X,Y)$ have a Y^{10} term that involves $\tau(q)$, these non-elementary contributions cancel out, leaving counts for $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ that are polynomial in q.

We have 11 constraints given by the Y^j coefficient of $W^{DP}_{C'_{2,4}}(X+(q-1)Y, X-Y)$ for each $j \in [0,10]$ and 8 unknowns a_j for $j \in [0,7]$. It is easy to see that not every dual coefficient gives a new constraint. For example, the fact that the Y^1 coefficient is 0 is implied by the condition that $a_j = a_{-j}$. The fact that these constraints are not independent is one of the key differences between this computation and the analogous one for del Pezzo surfaces of degree 3.

For each $j \in [1,7]$ we consider the Taylor series expansion of

$$((X+(q-1)Y)^{q^2+q+1-qj}(X-Y)^{q^3-qj-1} + (X+(q-1)Y)^{q^2+q+1+qj}(X-Y)^{q^3+qj-1}$$

in the variable Y. The Y^1 term is equal to 0, but we use Y^0 and then Y^k for $k \in [2,10]$ to create a column vector for each j with 10 entries. For $j=0$ we consider the expansion of $(X+(q-1)Y)^{q^2+q+1}(X-Y)^{q^3-1}$, again omitting the Y^1 term. The rows of the resulting matrix correspond to increasing powers of Y.

We multiply this 10×8 matrix by a column vector with entries $a_0, a_1, \ldots, a_7$ and try to solve the matrix equation where this is equal to the column vector with entries given by Corollary 65. One would hope that this system of linear equations in the a_j is uniquely determined; that is what happens in the analogous computation for cubic surfaces. Unfortunately, a computation shows that this matrix only has rank 6.

Therefore, if we can find the values of a_7 and a_6 we can adjust this matrix equation and hope for a unique solution. This gives a modified version of the column vector with entries given by Corollary 65 consisting only of the contribution to these values from $a_0, \ldots, a_5$. Once we have solved for a_6 and a_7, this will give a system where we multiply a 10×6 matrix by a column vector with entries, $a_0, a_1, \ldots, a_5$ and get this modified version of the vector with entries from Corollary 65 as the result. This

matrix has rank 6 and we get a unique solution. This solution is the content of Theorem 3.

For the particular case $q = 5$ we get

$$a_7 = a_6 = 0,\ a_5 = 7750,\ a_4 = 2728000,\ a_3 = 119977750,$$

$$a_2 = 1646534000,\ a_1 = 7426406500,\ a_0 = 12125699601.$$

This matches our direct computation of the weight distribution of the 5^{16} elements of the code $C'_{2,4}$ over $\mathbb{F}_5$. This took over a day of computing time and is the last case where this computation is feasible using our current implementation. Later in this chapter we return to this example and explain the value $a_5 = 7750$. We also study these counts for other small values of q.

2. Del Pezzo Surfaces of Trace 7 and 6

The goal of this section is to give a proof of Theorem 27. First we consider the easier case of surfaces of trace 7. We show that these surfaces come from blowing up seven points in $\mathbb{P}^2(\mathbb{F}_q)$ in general position. We then count how many times each surface arises from blowing up such a 7-tuple. Next, we show that surfaces of trace 6 come from blowing up seven points in $\mathbb{P}^2(\mathbb{F}_q)$ in near general position. Given such a weak del Pezzo surface $\overline{S}$ we study $\mathrm{Pic}(\overline{S})$ to determine the number of ways $\overline{S}$ arises from blowing up seven such points. In this case, the lattice generated by (-2)-curves of $\overline{S}$ is one-dimensional, so we must study the action of the Weyl group of E_7 on $\mathrm{Pic}(\overline{S})$ in more detail.

Let $\overline{S}$ be a weak del Pezzo surface of degree 2. By Proposition 24, the number of $\mathbb{F}_q$-rational solutions of the anti-canonical model of $\overline{S}$ is $q^2 + q + 1 + tq$, where

$$t = \mathrm{Tr}(\varphi|_{E_7}) - \mathrm{Tr}(\varphi|_{\mathcal{R}}) = \mathrm{Tr}(\varphi|_{\mathcal{R}^\perp}),$$

φ is the Frobenius endomorphism and $\mathcal{R}$ is the sublattice of $\mathrm{Pic}(S)$ generated by (-2)-curves. Since $\mathrm{Tr}(\varphi|_{E_7})$ takes values between -7 and 7, but not ± 6, and t is bounded in absolute value by $\dim(\mathcal{R}^{\perp})$, we see that $t = 7$ if and only if $\mathcal{R}$ is trivial and $\mathrm{Tr}(\varphi|_{E_7}) = 7$. Moreover, we see that $t = 6$ implies that $\mathcal{R}$ is one-dimensional. Since $\mathcal{R}$ is a root lattice, it is isomorphic to A_1.

In order to determine a_7 and a_6 we give some information about the $2:1$ map $\phi:\ \overline{S} \to \mathbb{P}^2$. Suppose that $\overline{S}$ is the blow-up of points $p_1, \ldots, p_7$ in $\mathbb{P}^2(\mathbb{F}_q)$. We would like to determine how many equations of the form $w^2 = f_4(x, y, z)$ arise from $\overline{S}$. We recall some facts from Proposition 11. There is a 3-dimensional space of cubics vanishing at $p_1, \ldots, p_7$. We choose a basis for this space, and call these cubics x, y, z. We can choose these coordinates in $|\mathrm{PGL}_3(\mathbb{F}_q)|$ ways.

There is a 7-dimensional space of sextic polynomials vanishing to order 2 at each p_i. Any such sextic w not in the space spanned by quadratic polynomials in x, y and z, $\langle x^2, xy, xz, y^2, yz, z^2 \rangle$, satisfies an equation of the form

$$w^2 - w \cdot f_2(x, y, z) - f_4(x, y, z) = 0,$$

where $f_2(x, y, z)$ is quadratic, and $f_4(x, y, z)$ is a homogeneous quartic. We want a sextic for which the polynomial $f_2(x, y, z)$ is zero. This gives six linear conditions, leading to a 1-dimensional space. We must not choose $w = 0$, so we have $q-1$ choices for w.

We recall that the number of 7-tuples of points in $\mathbb{P}^2(\mathbb{F}_q)$ in general position is given by $S(q)|\mathrm{PGL}_3(\mathbb{F}_q)|$ and the number of 7-tuples in near general position is given by $R(q)|\mathrm{PGL}_3(\mathbb{F}_q)|$.

We now give the proof of the trace 7 case.

PROOF. A weak del Pezzo surface with $q^2 + q + 1 + 7q$ points is the blow-up of seven $\mathbb{F}_q$-points of $\mathbb{P}^2(\mathbb{F}_q)$ in general position. Consider the surfaces we get by blowing

up all such 7-tuples. We saw in the previous paragraph that one such 7-tuple gives rise to $|\mathrm{GL}_3(\mathbb{F}_q)|$ quartics $w^2 = f_4(x, y, z)$.

A homogeneous quartic $w^2 = f_4(x, y, z)$ with $q^2 + q + 1 + 7q$ $\mathbb{F}_q$-points is the anti-canonical model of a smooth del Pezzo surface S. We want to know the number of blowing-down structures of this surface. The 28 bitangent lines of the branch quartic $f_4(x, y, z)$ are the images of the (-1)-curves of S under ϕ. The quartic restricted to one of these lines is a perfect square. Choosing a value of w is equivalent to choosing which square root we take on such a quartic. Taking seven pairwise-skew (-1)-curves on S gives a geometric basis $\{H, e_1, \ldots, e_7\}$ for $\mathrm{Pic}(S)$. Because the divisor classes must satisfy $e_i \cdot e_j = 0$ for $i \neq j$, we cannot choose these square roots arbitrarily for each bitangent.

Blowing up each tuple in general position and choosing coordinates for the anti-canonical model of the resulting surface gives

$$|\mathrm{PGL}_3(\mathbb{F}_q)|S(q)|\mathrm{GL}_3(\mathbb{F}_q)|$$

homogeneous quartics $w^2 = f_4(x, y, z)$. However, we have over-counted. A surface S arises as the blow-up of more than one 7-tuple.

Starting from a tuple $p_1, \ldots, p_7$, blowing up gives a surface S and a canonical root basis for $\mathrm{Pic}(S)$, or equivalently, a blowing-down structure for S. Starting with an equation of the form $w^2 = f_4(x, y, z)$ with $f_4(x, y, z)$ smooth, we can find the bitangents of the quartic and take the preimages under this ϕ. Any set of seven pairwise disjoint (-1)-curves gives a canonical root basis for $\mathrm{Pic}(S)$, or equivalently, a blowing-down structure of S. We have seen that the Weyl group of E_7 acts simply transitively on these canonical root bases, so the number of blowing-down structures of S is equal to $|W(E_7)|$.

The smooth surface S arises as the blow-up of seven points in general position in exactly $|W(E_7)|$ ways. A blowing-down structure gives points in $\mathbb{P}^2(\mathbb{F}_q)$, $p_1, \ldots, p_7$,

but it does not give a canonical choice of coordinates for this space. There are $|\mathrm{PGL}_3(\mathbb{F}_q)|$ choices for these coordinates. Therefore, we get

$$a_7 = \frac{|\mathrm{PGL}_3(\mathbb{F}_q)|S(q)|\mathrm{GL}_3(\mathbb{F}_q)|}{|\mathrm{PGL}_3(\mathbb{F}_q)||W(E_7)|},$$

completing the proof of the statement for a_7. □

We now turn to the more complicated case, surfaces of trace 6.

Proof. Given a weak del Pezzo surface S of degree 2, the number of points on the anti-canonical model of S is $q^2+q+1+tq$, for $t = \mathrm{Tr}(\varphi|_{E_7}) - \mathrm{Tr}(\varphi|_{\mathcal{R}})$, where $\mathcal{R}$ is the sublattice of E_7 generated by the (-2)-curves of S. We have seen above that if $t = 6$, then $\mathcal{R}$ is one-dimensional and $\mathrm{Tr}(\varphi|_{E_7}) = 7$. So there is a unique (-2)-curve of S. Since $\mathcal{R}$ is a root sublattice of E_7, it is isomorphic to A_1. All sublattices A_1 are equivalent under automorphisms of E_7.

Given any geometric basis of $\mathrm{Pic}(S)$, $\{H, e_1, \ldots, e_7\}$, consider the divisor class $D = 2H - (e_1 + \cdots e_6)$. This satisfies

$$D \cdot D = 4H \cdot H + \sum_{i=1}^{6} e_i \cdot e_i = 4 - 6 = -2.$$

Recall that the anti-canonical class is given by

$$K = 3H - (e_1 + \cdots + e_7),$$

and that the orthogonal complement of K in $\mathrm{Pic}(S)$ is isomorphic to E_7. It is easy to verify that $D \cdot K = 0$. Since D has norm -2 this divisor class generates an A_1 sublattice in E_7. By taking an automorphism of E_7 we may suppose that the sublattice $\mathcal{R}$ generated by the (-2)-curve of S is generated by D. Blowing up a 7-tuple of points $p_1, \ldots, p_7$ in near general position gives a weak del Pezzo surface S with a geometric basis such that D is the class of the (-2)-curve on S exactly when $p_1, \ldots, p_6$ lie on a conic not containing p_7. This is the case for exactly $1/7$ of the

7-tuples in near general position. The orthogonal complement of A_1 in E_7 is D_6. The direct sum $A_1 \oplus D_6$ is contained in E_7 with index 2. The presence of this (-2)-curve gives this decomposition.

We now determine how many blowing-down structures for S give a 7-tuple in near general position. Suppose we have a geometric basis $\{H, e_1, \ldots, e_7\}$ for $\mathrm{Pic}(S)$ and a sublattice A_1 generated by the divisor $D = 2H - (e_1 + \cdots e_6)$. Let $r_i = e_i - \frac{K}{2}$. Then

$$r_i \cdot K = e_i \cdot K - \frac{K \cdot K}{2} = 0.$$

We also have

$$r_i \cdot r_j = \left(e_i - \frac{K}{2}\right) \cdot \left(e_j - \frac{K}{2}\right) = -\delta_{ij} - 1 + \frac{K \cdot K}{4} = -\delta_{ij} - \frac{1}{2}.$$

These r_i are not in E_7 because they are not in the integer span of our basis, but they are in the dual lattice, E_7^*.

We note that $E_7 \subset E_7^*$ with index 2. We consider the orthogonal complement of A_1 in E_7^*. This contains the D_6 in E_7 with index 2. This orthogonal complement in E_7^* is contained in this $D_6^* \subset E_7^*$ with index 2. We can verify these index statements by computing discriminants of the relevant lattices. This gives the following picture:

$$\begin{array}{ccccc} E_7 & \subset & E_7^* & & \\ \cup & & \cup & & \\ A_1^\perp = D_6 & \subset & A_1^\perp \text{ in } E_7^* & \subset & D_6^* \end{array}.$$

The class r_7 is distinguished from $r_1, \ldots, r_6$ by its intersection with D. We have $r_7 \cdot D = 0$ and $r_i \cdot D = e_i \cdot D - \frac{K \cdot D}{2} = 1$ otherwise. We see that $(r_i + \frac{D}{2}) \cdot D = 0$ for $i \in [1, 6]$. Therefore, we have 7 vectors

$$\left\{r_7, r_1 + \frac{D}{2}, \ldots, r_6 + \frac{D}{2}\right\}$$

in E_7^* and r_7 in the orthogonal complement of A_1. The group D_6^*/D_6 is of order 4. Each vector $r_i + \frac{D}{2}$ is in the same coset of the group since

$$\left(r_i + \frac{D}{2}\right) - \left(r_j + \frac{D}{2}\right) = r_i - r_j = e_i - e_j,$$

and $e_i - e_j$ is orthogonal to both K and D. Vectors in one coset of this group have even integer norm and another coset consists of vectors with odd integer norm. So, $r_1, \ldots, r_6$ are in one of the two remaining cosets.

We determine this coset by considering the sum:

$$\begin{aligned}\sum_{i=1}^{6}\left(r_i + \frac{D}{2}\right) &= 6H - 3(e_1 + \cdots + e_6) - 3K + 3\sum_{i=1}^{7} e_i \\ &= -3H + 3e_7 + (e_1 + \cdots + e_6) \\ &= -K + 2e_7 = 2r_7.\end{aligned}$$

Half the sum of these divisors is in the same coset as r_7. Each $r_i + \frac{D}{2}$ has norm $-\frac{3}{2}$ and they are pairwise orthogonal. This gives an orthonormal frame for $\mathbb{Z}^6 \subset D_6^*$. There are $2^6 \cdot 6!$ ways to choose such an orthonormal frame for $\mathbb{Z}^6$, but we are not completely free to choose the signs for each of these six elements. The condition on the coset of their sum implies that once we have chosen five signs, the sixth is determined. This gives $2^5 \cdot 6!$ choices for such a frame. We compute that $\frac{|W(E_7)|}{2^5 \cdot 6!} = 126$.

The Weyl group of E_7 no longer acts transitively on canonical root bases. Instead, we see that each weak del Pezzo surface that is the blow-up of some 7-tuple in near general position has $\frac{|W(E_7)|}{126}$ blowing-down structures corresponding to a 7-tuple in near general position. For each such blowing-down structure we also choose coordinates for the $\mathbb{P}^2(\mathbb{F}_q)$ containing these points.

Blowing up all 7-tuples in near general position such that $p_1, \ldots, p_6$ lie on a conic not containing p_7 and then choosing coordinates for the $2:1$ map to $\mathbb{P}^2$ gives

$$|\mathrm{PGL}_3(\mathbb{F}_q)|\frac{R(q)|\mathrm{GL}_3(\mathbb{F}_q)|}{7}$$

homogeneous quartics $w^2 = f_4(x,y,z)$ with q^2+7q+1 solutions in $\mathbb{P}(2,1,1,1)$. Given such a quartic there are $2^5 \cdot 6!|\mathrm{PGL}_3(\mathbb{F}_q)|$ blowing-down structures that give a 7-tuple in near general position. Dividing gives

$$a_6 = \frac{18|\mathrm{GL}_3(\mathbb{F}_q)|R(q)}{|W(E_7)|},$$

completing the proof. □

Finally, we must compute $S(q)$ and $R(q)$. We begin with a discussion of k-arcs in $\mathbb{P}^2(\mathbb{F}_q)$. A subset of points $S \subset \mathbb{P}^2(\mathbb{F}_q)$ is called an *arc* if no three points of S lie on a line. A *k-arc* is a collection of k distinct points that form an arc. It is elementary to give a count for k-arcs for k up to 6. For example, suppose $p_1, \ldots, p_5$ form a 5-arc. There are $\binom{5}{2} = 10$ distinct lines between these points. Each line contains two of these five points and $q-1$ other points. It is not difficult to show that there are $10q-20$ distinct points on these lines. Therefore, given a 5-arc there are $q^2-9q+21$ choices of another point of $\mathbb{P}^2(\mathbb{F}_q)$ so that the resulting collection forms a 6-arc. This count is independent of the choice of 5-arc. The following counts for k-arcs are given in Theorem 4.1 of [**23**].

Proposition 66. *Let $A(k,q)$ denote the number of k-arcs in $\mathbb{P}^2(\mathbb{F}_q)$. Then*

$$A(1,q) = q^2+q+1, \qquad A(2,q) = \frac{A(1,q)(q^2+q)}{2},$$
$$A(3,q) = \tfrac{A(2,q)q^2}{3}, \qquad A(4,q) = \frac{A(3,q)(q-1)^2}{4},$$
$$A(5,q) = \tfrac{A(4,q)(q-2)(q-3)}{5}, \quad A(6,q) = \frac{A(5,q)(q^2-9q+21)}{6}.$$

Counting 7-arcs leads to new difficulties. Starting with a 6-arc $\{p_1, \ldots, p_6\}$, the number of choices of p_7 leading to a 7-arc depends on the choice of $\{p_1, \ldots, p_6\}$. This is also the first case where the count is not a polynomial in q. The function $A(7, q)$ is a polynomial in q plus a term involving the number of copies of $\mathbb{P}^2(\mathbb{F}_2)$ in $\mathbb{P}^2(\mathbb{F}_q)$, which is zero if the characteristic of $\mathbb{F}_q$ is not equal to 2. Therefore, $A(7, q)$ is a polynomial in q as long as we exclude characteristic 2. For details, see [**23**]. The following result is Theorem 4.2 of that paper.

Proposition 67. *Let* (7_3) *denote the number of copies of* $\mathbb{P}^2(\mathbb{F}_2)$ *in* $\mathbb{P}^2(\mathbb{F}_q)$. *Then*

$$\begin{aligned} A(7,q) &= \frac{1}{7!}(q^2+q+1)(q+1)q^3(q-1)^2(q-3)(q-5) \\ &\times \quad (q^4-20q^3+148q^2-468q+498)-(7_3). \end{aligned}$$

In order to compute $S(q)$ we need to understand how many of these 7-arcs satisfy the additional condition that no six points lie on a conic. It is easy to count the number of collections of seven points that lie on a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$. This is the number of smooth conics, $q^5 - q^2$, times $\binom{q+1}{7}$. We call this quantity $C_7(q)$. It follows that $A(7, q) = S(q) + R(q) + C_7(q)$, giving

$$S(q)+R(q) = \frac{1}{7!}(q^2+q+1)(q^2+q)q^2(q-1)^2(q-3)(q-5)(q-7)(q^3-13q^2+56q-70).$$

The factor of $(q^2 + q + 1)(q^2 + q)q^2(q - 1)^2 = |\mathrm{PGL}_3(\mathbb{F}_q)|$ comes from fixing the first four points of the configuration. We find $R(q)$ and subtract to get $S(q)$.

Lemma 68. *We have*

$$S(q) = (q-7)(q-5)(q-3)(q^3-20q^2+119q-175),$$

and that

$$R(q) = 7(q-7)(q-5)(q-3)(q^2-9q+15).$$

PROOF. There are q^5-q^2 smooth conics in $\mathbb{P}^2(\mathbb{F}_q)$, all equivalent under $\mathrm{PGL}_3(\mathbb{F}_q)$. We fix one such conic C and count collections of points $p_1,\ldots,p_6$ on C and p_7 not on C such that $\{p_1,\ldots,p_7\}$ form a 7-arc. We first consider the number of choices of p_7. For any $p_7 \notin C$, there are two tangent lines to C passing through it. They are either both rational, or are Galois-conjugate. There are q^2 points not on C, $\frac{q(q+1)}{2}$ of which lie on two $\mathbb{F}_q$-rational tangent lines to C. The other $\frac{q(q-1)}{2}$ points lie on two Galois-conjugate tangent lines.

First suppose that p_7 does not lie on any $\mathbb{F}_q$-rational tangent line. Then the line between any $\mathbb{F}_q$-point p of C and p_7 passes through one other $\mathbb{F}_q$-point of C, which we call p'. If both p and p' are in $\{p_1,\ldots,p_6\}$ then $\{p_1,\ldots,p_7\}$ is not a 7-arc. So, the $q+1$ rational points of C split into $\frac{q+1}{2}$ pairs. We choose six of these pairs and one point of each pair, giving $2^6\binom{\frac{q+1}{2}}{6}$ sets $\{p_1,\ldots,p_6,p_7\}$ forming a 7-arc.

Now suppose that p_7 lies on two $\mathbb{F}_q$-rational tangent lines. Each point of tangency is an $\mathbb{F}_q$-point of C. The remaining $\frac{q-1}{2}$ points of C are paired as in the previous paragraph. We can choose either $0, 1$, or 2 of the points of tangency on the lines through p_7 to be in the set $\{p_1,\ldots,p_6\}$. We then must pick the remaining points from the $\frac{q-1}{2}$ pairs of points of C that do not include the two points of tangency. This gives

$$2^6\binom{\frac{q-1}{2}}{6} + 2\cdot 2^5\binom{\frac{q-1}{2}}{5} + 2^4\binom{\frac{q-1}{2}}{4}$$

choices of the 6 points of C. We call this quantity N and see that

$$|\mathrm{PGL}_3(\mathbb{F}_q)|R(q) = 7(q^5-q^2)\left(\frac{q(q-1)}{2}2^6\binom{\frac{q+1}{2}}{6} + \frac{q(q+1)}{2}N\right),$$

completing the proof. □

Similar computations let us to determine the analogous counts for even values of q. We omit this case because we have assumed that the characteristic of $\mathbb{F}_q$ is odd earlier in this thesis.

3. Examples of Surfaces of Maximal Trace for Small q

In this section we consider the consequences of the counts given in Theorem 3 for small values of q. We let

$$T_7(q) = \frac{2S(q)}{|W(E_7)|} = \frac{2(q-7)(q-5)(q-3)(q^3-20q+119q-175)}{|W(E_7)|}.$$

We see that $T_7(q) = 0$ for all odd $q < 9$ because there are no configurations of 7 points in general position in $\mathbb{P}^2(\mathbb{F}_q)$ for $q \leq 7$. For $q = 9$ there is such a configuration. In fact, $T_7(q) = 240$. This is small enough that we can classify such configurations and completely understand del Pezzo surfaces of degree 2 over $\mathbb{F}_q$ with an anti-canonical model that has the maximum number of points, $q^2 + 8q + 1$. We say that a del Pezzo surface of degree 2 with this number of points has maximal trace.

Before focusing on particular values of q, we give a more general discussion of how a single equation of the form $w^2 = f_4(x, y, z)$ affects the count for $T_7(q)$. Let C be the curve in $\mathbb{P}^2(\mathbb{F}_q)$ defined by $f_4(x, y, z) = 0$. After choosing coordinates, there are $|\mathrm{PGL}_3(\mathbb{F}_q)|/|\mathrm{Aut}(C)|$ quartics $f_4(x, y, z)$ that give a curve isomorphic to C. There is a factor of $q - 1$ that comes from considering scalings of w.

Suppose that $w^2 = f_4(x, y, z)$ is the anti-canonical model of a smooth del Pezzo surface S. The Weyl group of E_7 acts transitively on the 7-tuples of pairwise disjoint (-1)-curves of S. Choose seven such (-1)-curves and consider their image under the $2:1$ map ϕ. This gives 7 bitangents of the quartic $f_4(x, y, z)$.

We claim that there are $|W(E_7)|/2$ possible collections of 7 points in $\mathbb{P}^2(\mathbb{F}_q)$ that blow up to this surface. This is because $-1 \in W(E_7)$ and switching $-w$ and w on each of these 7 bitangent lines does not change the resulting configuration. Therefore, we have $|\mathrm{GL}_3(\mathbb{F}_q)|\frac{|W(E_7)|}{2|\mathrm{Aut}(C)|}$ surfaces that are equivalent to $w^2 = f_4(x, y, z)$ together with a choice of 7 pairwise disjoint (-1)-curves coming from proper transforms of the 7 points of the blow-up. Blowing down these lines gives a configuration of 7 points. This discussion gives the following result.

Lemma 69. *We have*

$$\sum_C \frac{1}{|\mathrm{Aut}(C)|} = T_7(q),$$

where the sum is taken over all non-isomorphic curves C given by $f_4(x,y,z)$ where $w^2 = f_4(x,y,z)$ is the anti-canonical model of a del Pezzo surface of maximal trace.

This argument works for more general counts for quartics on $\mathbb{P}(2,1,1,1)$ with trace t, that is, $w^2 = f_4(x,y,z)$ with $q^2+q+1+tq$ $\mathbb{F}_q$-points. Let $w^2 = f_4(x,y,z)$ have trace t, and suppose that the curve given by $f_4(x,y,z) = 0$ is smooth. Then this quartic contributes

$$|\mathrm{GL}_3(\mathbb{F}_q)|\frac{2}{|\mathrm{Aut}(C)||W(E_7)|}$$

to the overall count for surfaces of trace t.

Suppose that $f_4(x,y,z)$ defines a plane quartic with a single node and that $w^2 = f_4(x,y,z)$ is the anti-canonical model of a weak del Pezzo surface S. Then the lattice $\mathcal{R}$ generated by the (-2)-curves of S is one-dimensional. In this case, the quartic $f_4(x,y,z)$ contributes

$$|\mathrm{GL}_3(\mathbb{F}_q)|\frac{252}{|\mathrm{Aut}(C)||W(E_7)|}$$

to the overall count of surfaces of trace t. The extra factor of 126 accounts for the fact that the Weyl group of E_7 no longer acts transitively on 7-tuples of pairwise disjoint (-1)-curves of S. For surfaces with more complicated singular lattices, or equivalently quartics with other types of singularities, we could determine the relevant contribution to the total count for surfaces of trace t, but we will not need this here.

This gives a strategy for classifying all quartics $f_4(x,y,z)$ over a fixed $\mathbb{F}_q$ for which $w^2 = f_4(x,y,z)$ has trace t in the case where all such quartics are either smooth or have a single node. This is somewhat similar to mass formulas for lattices. From our computation of the total number of quartics such that $w^2 = f_4(x,y,z)$ has trace t we know the result when we sum over the size of the automorphism groups of these

quartics. We need only find enough non-isomorphic quartics that the sum of the reciprocals of the orders of their automorphism groups gives this value. When these terms add up to the desired count, we know that there are no other quartics left to find. We apply this approach for several small values of q.

We will see that for small values of q several of the curves giving the anti-canonical model of a del Pezzo surface of degree 2 of maximal trace are highly symmetric and have many automorphisms. Below we give a process to find the a quartic $f_4(x, y, z)$ coming from the blow-up of a 7-tuple in general position. We often find a quartic $f_4(x, y, z)$ through this process with somewhat complicated coefficients, and then after finding the automorphism group can give an isomorphic quartic that is simpler. The number of automorphisms of a curve C defined over $\mathbb{C}$ will be equal to the number of automorphisms of the reduction of this curve over $\mathbb{F}_q$, except in some exceptional cases, such as the reduction of the Klein quartic over $\mathbb{F}_9$. Therefore, in order to find a nice model of a curve over $\mathbb{F}_q$ with a particular large number of automorphisms, 24 for example, we start by considering the reductions of plane quartic curves with 24 automorphisms over $\mathbb{C}$. A list of smooth plane quartic curves $C/\mathbb{C}$ with large $\mathrm{Aut}(C)$ is given in [**2**]. We use this list throughout this section to find nicer models for the curves that we discover.

Much of the work in this section involves computing the automorphism groups of plane quartics over finite fields. The computer algebra system Magma has built-in commands to compute automorphism groups of curves over finite fields and to check whether two curves are isomorphic [**6**].

Proposition 70. *There is a unique degree* 2 *del Pezzo surface of maximal trace over* $\mathbb{F}_9$. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_9)$, *its anti-canonical model is given by*

$$w^2 = x^4 + y^4 + z^4.$$

The curve $f_4(x, y, z) = x^4 + y^4 + z^4$ is known as the Fermat quartic.

PROOF. It is straightforward to see that $w^2 = x^4+y^4+z^4$ has $9^2+8\cdot 9+1$ $\mathbb{F}_q$-points over $\mathbb{F}_9$. It is also well known that the Fermat quartic has 6048 automorphisms defined over $\mathbb{F}_9$. A computation in Magma verifies the size of the automorphism group. We see that $T_7(9) = \frac{1}{6048}$, completing the proof. $\square$

In this case one might guess that the Fermat quartic gives the anti-canonical model of a surface of maximal trace. Computing $T_7(9)$ shows that all homogeneous quartics $w^2 = f_4(x, y, z)$ with trace 7 come from automorphisms of the Fermat quartic. For values $q > 9$ it will not be so easy to guess the curves that give anti-canonical models of surfaces of maximal trace.

We explain how to go from a 7-tuple of points in $\mathbb{P}^2(\mathbb{F}_q)$ to the $w^2 = f_4(x, y, z)$ model of the del Pezzo surface of degree 2 obtained from blowing up these points. This is the content of Proposition 11.

Given 7 points in $\mathbb{P}^2(\mathbb{F}_q)$ there is a 3-dimensional space of cubic polynomials vanishing at each of them. We choose a basis for this space of cubics. Taking quadratic polynomials in the polynomials of this basis gives a 6-dimensional space of sextic polynomials vanishing to degree 2 at each of these 7 points. We consider the space of sextic polynomials with this property. There is a 28-dimensional space of sextics on $\mathbb{P}^2(\mathbb{F}_q)$. Vanishing to degree 2 at a point imposes three independent conditions. For example, for a sextic polynomial to vanish to degree 2 at $[0 : 0 : 1]$ the z^6, xz^5, and yz^5 coefficients must all be 0. For points in general position these conditions are independent, giving a $28 - 21 = 7$ dimensional space of sextic polynomials vanishing to degree 2 at each point.

There are q^7-q^6 sextic polynomials satisfying this property that cannot be written as a quadratic in the three cubics found earlier. Let $T(x, y, z)$ be one such sextic. This polynomial satisfies a quadratic relation in the cubics we found earlier. That is,

$$T(x, y, z)^2 + T(x, y, z)f_2(c_1, c_2, c_3) + f_4(c_1, c_2, c_3) = 0,$$

where c_1, c_2 are c_3 are a basis for the space of cubics vanishing on these seven points, $f_2(x, y, z)$ is a quadratic polynomial, and $f_4(x, y, z)$ is a quartic. We find the equation $w^2 + wf_2(x, y, z) + f_4(x, y, z) = 0$. Completing the square gives an equation of the form $w^2 = f_4(x, y, z)$.

We will demonstrate this process starting with a 7-tuple in general position over $\mathbb{F}_9$. The previous proposition implies that the end result will be an equation of the form $w^2 = f_4(x, y, z)$ where $f_4(x, y, z)$ is isomorphic to the Fermat quartic. Let a be defined so that $a^2 - a - 1 = 0$ in $\mathbb{F}_9$. The element of $\mathbb{F}_9$ are $\{0, 1, 2, a, a+1, a+2, 2a, 2a+1, 2a+2\}$. Now let

$$p_1 = [1 : 0 : 0],\ p_2 = [0 : 1 : 0],\quad p_3 = [0 : 0 : 1],$$
$$p_4 = [1 : 1 : 1],\ p_5 = [2 : a : 1],\quad p_6 = [a+1 : 2a+1 : 1],\ p_7 = [2a+2 : 2 : a].$$

It is not difficult to check that these 7 points are in general position. For example, a 3×3 matrix with rows corresponding to the entries of p_i, p_j, p_k will have determinant 0 if and only if these points are collinear. Evaluating coordinates at monomials of degree 2 gives a row vector with 6 elements, and checking whether 6 points lie on a conic is equivalent to checking the non-vanishing of a 6×6 determinant.

The three dimensional space of cubics vanishing on these points is generated by

$$\begin{aligned} c_0(x, y, z) &= x^2y + (2a+1)\ xyz + 2\,xz^2 + 2a\,y^2z + (2a+2)\ yz^2 \\ c_1(x, y, z) &= x^2z + (2a+2)\ xyz + (a+1)\ xz^2 + 2\,y^2z \\ c_2(x, y, z) &= xy^2 + 2a\,xyz + (a+1)\ xz^2 + y^2z. \end{aligned}$$

A similar, but more complicated, linear algebra calculation finds that the 7-dimensional space of sextics vanishing to order 2 at each of $p_1, \ldots, p_7$ is generated by

the six quadratic monomials in c_0, c_1, c_2 together with

$$\begin{aligned} h(x,y,z) &= x^4y^2 + 2\,x^3yz^2 + 2a\,x^2y^3z + (a+1)\;x^2yz^3 + (2a+2)\;x^2z^4 + 2\,xy^4z \\ &\quad + a\,xy^2z^3 + a\,xyz^4 + a\,y^3z^3 + (a+1)\;y^2z^4. \end{aligned}$$

Interpolating at many points in $\mathbb{P}^2(\mathbb{F}_9)$ suggests the quadratic relation satisfied by $h(x,y,z)$ and the six quadratic monomials in c_0, c_1, c_2. We verify that the following identity holds:

$$\begin{aligned} &(2a+2)\;x^4 + x^3y + a\,x^3z + 2a\,x^2y^2 + (a+2)\;x^2yz + (a+2)\;x^2z^2 + (2a+1)\;xy^2z \\ &+2\,xyz^2 + (a+2)\;y^2z^2 + (a+2)\;yz^3 + a\,wx^2 + 2\,wxy + 2a\,wxz + a\,wy^2 + a\,wyz \\ &+ (2a+1)\,wz^2 + w^2 = 0, \end{aligned}$$

where $w = h(x,y,z),\ x = c_0(x,y,z),\ y = c_1(x,y,z)$ and $z = c_2(x,y,z)$. Completing the square gives

$$\begin{aligned} w^2 &= (a+1)\;x^4 + (2a+1)\;x^3y + 2\,x^3z + 2a\,xy^3 + xz^3 \\ &\quad + (2a+2)\;y^4 + (a+1)\;y^3z + (a+1)\;yz^3 + (a+1)\;z^4. \end{aligned}$$

A computation in Magma gives an explicit isomorphism between the quartic on the right-hand side of this equation and the Fermat quartic.

We apply this type of analysis for other small values of q.

Proposition 71. *There is a unique degree* 2 *del Pezzo surface of maximal trace over* $\mathbb{F}_{11}$. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_{11})$, *it has anti-canonical model given by* $w^2 = f_4(x,y,z)$, *where*

$$f_4(x,y,z) = x^4 + y^4 + z^4 + (x^2y^2 + x^2z^2 + y^2z^2),$$

a form of the Klein quartic over $\mathbb{F}_{11}$.

PROOF. We check this this homogeneous quartic in $\mathbb{P}(2,1,1,1)$ is the anti-canonical model of a surface with maximal trace and that the curve $f_4(x,y,z)=0$ has 168 automorphisms. The computed value of $T_7(q)$ shows that this accounts for all maximal surfaces. □

Starting with a 7-tuple of points in $\mathbb{P}^2(\mathbb{F}_{11})$ in general position leads to a different quartic. Magma computes that it has 168 automorphisms. Once we know that there is exactly one isomorphism class of curve C contributing to this count, and that it has this many isomorphisms, we find a model of the Klein quartic, the unique curve with 168 automorphisms over $\mathbb{C}$, where these automorphisms are all defined over $\mathbb{F}_{11}$. This model of the Klein quartic exists because $\mathbb{F}_{11}$ contains a square root of -7 [**21**].

The first case where there exist non-isomorphic maximal trace del Pezzo surfaces of degree 2 is over $\mathbb{F}_{13}$. However, we cannot predict this from the value $T_7(13)=\frac{1}{16}$. It turns out that there is no plane quartic $f_4(x,y,z)$ with 16 automorphisms such that $w^2=f_4(x,y,z)$ is the anti-canonical model of a maximal trace del Pezzo surface, but we did not know this a priori.

Proposition 72. *There are two distinct isomorphism classes of del Pezzo surface of degree* 2 *over* $\mathbb{F}_{13}$ *with maximal trace. Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_{13})$ *the anti-canonical models of these surfaces are given by* $w^2=f_j(x,y,z)$ *with*

$$\begin{aligned} f_1(x,y,z) &= x^4+y^4+z^4+8(x^2y^2+x^2z^2+y^2z^2) \\ f_2(x,y,z) &= x^4+y^4+z^4-x^2y^2. \end{aligned}$$

The quartic $f_1(x,y,z)$ *has* 24 *automorphisms and the quartic* $f_2(x,y,z)$ *has* 48 *automorphisms.*

PROOF. We note that $\frac{1}{24}+\frac{1}{48}=T_7(q)$. By choosing collections of seven points in general position and going through the process described above we found two quartics

$g_j(x,y,z)$ giving anti-canonical models of surfaces of maximal trace:

$$\begin{aligned} g_1(x,y,z) &= 10x^4+6x^3y+4x^3z+6x^2y^2+3x^2yz+12x^2z^2+4xy^3+7xy^2z+12xyz^2 \\ &\quad +7xz^3+3y^4+y^3z+5y^2z^2+4yz^3+3z^4, \\ g_2(x,y,z) &= 10x^4+2x^3y+2x^3z+9x^2y^2+5x^2yz+5x^2z^2\ +7xy^3+11xy^2z \\ &\quad +12xyz^2+4xz^3+12y^4+6y^3z+8y^2z^2+11yz^3+z^4. \end{aligned}$$

A computation in Magma shows that $g_1(x,y,z)$ has 24 automorphisms and that $g_2(x,y,z)$ has 48 automorphisms.

The quartic $x^4+y^4+z^4+8(x^2y^2+x^2z^2+y^2z^2)$ has 24 automorphisms as a curve over $\mathbb{C}$ [**2**]. This suggested checking whether it gives a surface of maximal trace, and it is easy to verify that it does. A computation in Magma gives an isomorphism between this curve and $g_1(x,y,z)$.

The quartic $x^4+y^4+z^4+2\sqrt{-3}x^2y^2$ has 48 automorphisms over $\mathbb{C}$ [**36**]. We check that this quartic gives the anti-canonical model of a surface of maximal trace, and that its reduction to $\mathbb{F}_{13}$ is isomorphic to $g_2(x,y,z)$. □

Over $\mathbb{F}_{17}$ we know that there will not be a unique del Pezzo surface of maximal trace up to isomorphism. This is because $T_7(17)=\frac{109}{96}$ does not have a unit numerator. In fact, we find that there are many non-isomorphic classes of these maximal trace del Pezzo surfaces. A similar but larger calculation gives the following result.

Proposition 73. *There are seven non-isomorphic del Pezzo surfaces of degree* 2 *of maximal trace over* $\mathbb{F}_{17}$. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_{17})$, *the anti-canonical models of these surfaces are given by* $w^2=g_j(x,y,z)$ *where:*

$$\begin{aligned} g_1(x,y,z) &= x^4+y^4+z^4 \\ g_2(x,y,z) &= x^4+6x^3y+6x^3z+3x^2y^2+15x^2yz+7x^2z^2-xy^3+12xy^2z+11xyz^2 \\ &\quad +11xz^3+9y^4+12y^3z+10y^2z^2+z^4 \end{aligned}$$

$$
\begin{aligned}
g_3(x,y,z) &= x^4+10x^3y+16x^2y^2+5x^2yz+14x^2z^2+6xy^3+16xy^2z+4xyz^2-y^4 \\
&\quad +14y^3z+14y^2z^2+yz^3+15z^4 \\
g_4(x,y,z) &= 2x^4+9x^3y+5x^3z+x^2y^2+6x^2yz+16x^2z^2+14xy^3+6xy^2z \\
&\quad +14xyz^2+6xz^3+4y^4+5y^3z+5y^2z^2+9yz^3+9z^4 \\
g_5(x,y,z) &= 15x^4+16x^3y+14x^3z+6x^2y^2+9x^2yz+13x^2z^2+xy^3+16xy^2z \\
&\quad +16xyz^2+9xz^3+15y^4+3y^3z+13y^2z^2+8yz^3+16z^4 \\
g_6(x,y,z) &= 9x^4+9x^3y+x^3z+8x^2y^2+2x^2yz+5x^2z^2+5xy^3+8xy^2z+13xyz^2 \\
&\quad +13xz^3+16y^4+4y^3z+15y^2z^2+7yz^3+8z^4 \\
g_7(x,y,z) &= 13x^4+12x^3y+13x^3z+11x^2y^2+12x^2yz+2x^2z^2+4xy^3+5xy^2z \\
&\quad +2xyz^2+10xz^3+9y^4+14y^3z+13y^2z^2+9yz^3+9z^4.
\end{aligned}
$$

The quartics $g_j(x,y,z)$ have $96, 24, 24, 8, 6, 4$, and 2 automorphisms, respectively.

We compute

$$T_7(17) = \frac{1}{96}+\frac{2}{24}+\frac{1}{8}+\frac{1}{6}+\frac{1}{4}+\frac{1}{2}.$$

We also note that we first found a different model of the curve with 96 automorphisms. A calculation shows that it is isomorphic to the Fermat quartic. We could similarly try to find a nicer model of the curves of 24 automorphisms, for example, but have not.

We note that $T_7(q)$ grows like a constant times q^6. It is an easy calculation to see that it is increasing for all $q \geq 7$ and that it is greater than 1 for all $q \geq 13$.

Proposition 74. *The only finite fields $\mathbb{F}_q$ of odd characteristic for which there is a unique degree 2 del Pezzo surface of maximal trace are $\mathbb{F}_9$ and $\mathbb{F}_{13}$.*

In fact, the number of isomorphism classes of surfaces of maximal trace grows quickly. The generic genus 3 curve has no non-trivial automorphisms, so as $q \to \infty$, we expect a constant times q^6 isomorphism classes of surfaces of maximal trace.

A more extensive calculation gives the classification of degree 2 del Pezzo surfaces of maximal trace over $\mathbb{F}_{19}$.

Proposition 75. *There are* 14 *non-isomorphic maximal del Pezzo surfaces of degree* 2 *over* $\mathbb{F}_{19}$. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_{19})$, *the anti-canonical models of these surfaces are given by* $w^2 = g_j(x, y, z)$ *where:*

$$\begin{aligned}
g_1(x,y,z) &= 16x^4 + 9x^3y + 10x^3z + 11x^2y^2 + 14x^2yz + 9xy^3 + 4xyz^2 + 3xz^3 \\
&\quad +16y^4 + 4y^3z + 17y^2z^2 + 17yz^3 + 6z^4 \\
g_2(x,y,z) &= 9x^4 + 4x^3y + 9x^3z + 18x^2y^2 + 10x^2yz + 5x^2z^2 + 10xy^3 + 9xy^2z \\
&\quad +2xyz^2 + 18xz^3 + 4y^4 + 9y^3z + 8y^2z^2 + 15yz^3 + 17z^4 \\
g_3(x,y,z) &= 11x^4 + 15x^3y + 11x^3z + 6x^2y^2 + 12x^2yz + 4x^2z^2 + 4xy^3 \\
&\quad +2xy^2z + 18xyz^2 + 3xz^3 + 11y^4 + 16y^3z + 16y^2z^2 + 5yz^3 + 6z^4 \\
g_4(x,y,z) &= 4x^4 + 15x^3y + 13x^3z + 13x^2y^2 + 3x^2yz + 16x^2z^2 + 13xy^3 \\
&\quad +10xy^2z + 4xyz^2 + 17xz^3 + 9y^4 + 15y^3z + 5y^2z^2 + 5yz^3 + 11z^4 \\
g_5(x,y,z) &= 7x^4 + 5x^3y + 17x^3z + x^2y^2 + 11x^2yz + x^2z^2 + 6xy^3 + 10xy^2z \\
&\quad +5xyz^2 + 15xz^3 + 4y^4 + 4y^3z + 7y^2z^2 + 10yz^3 + 9z^4 \\
g_6(x,y,z) &= 9x^4 + 13x^3y + 5x^3z + 13x^2y^2 + 12x^2yz + 8x^2z^2 + 15xy^3 \\
&\quad +10xy^2z + 7xyz^2 + 2xz^3 + 4y^4 + 2y^3z + 7y^2z^2 + 15yz^3 + 6z^4 \\
g_7(x,y,z) &= 5x^4 + 4x^3y + 17x^3z + 14x^2y^2 + 11x^2yz + 14x^2z^2 + 3xy^3 \\
&\quad +6xy^2z + 13xyz^2 + 17xz^3 + 4y^4 + 8y^3z + 18y^2z^2 + 14yz^3 + 5z^4
\end{aligned}$$

$$
\begin{aligned}
g_8(x,y,z) &= 6x^4+3x^3z+5x^2y^2+8x^2yz+10x^2z^2+18xy^2z+6xyz^2 \\
&\quad +3xz^3+5y^4+16y^3z+12y^2z^2+yz^3+6z^4 \\
g_9(x,y,z) &= 9x^4+14x^3y+11x^3z+11x^2y^2+16x^2yz+12x^2z^2+13xy^3 \\
&\quad +9xy^2z+14xyz^2+10xz^3+16y^4+7y^3z+14y^2z^2+4yz^3+z^4 \\
g_{10}(x,y,z) &= 16x^4+14x^3y+12x^3z+16x^2yz+5x^2z^2+2xy^3+16xy^2z \\
&\quad +9xyz^2+4xz^3+17y^4+15y^3z+6y^2z^2+11yz^3+6z^4 \\
g_{11}(x,y,z) &= x^4+7x^3y+15x^3z+13x^2y^2+2x^2yz+8x^2z^2+5xy^3+6xy^2z \\
&\quad +5xyz^2+11xz^3+4y^4+4y^3z+15y^2z^2+4z^4 \\
g_{12}(x,y,z) &= x^4+17x^3y+5x^3z+2x^2y^2+6x^2yz+16x^2z^2+18xy^3+10xy^2z \\
&\quad +16xyz^2+3xz^3+5y^4+2y^2z^2+11yz^3+11z^4 \\
g_{13}(x,y,z) &= 7x^4+x^3y+6x^3z+4x^2yz+15x^2z^2+11xy^3+11xy^2z \\
&\quad +6xyz^2+2xz^3+11y^4+9y^2z^2+11yz^3+5z^4 \\
g_{14}(x,y,z) &= 16x^4+2x^3y+10x^3z+16x^2y^2+8x^2yz+5x^2z^2+3xy^3 \\
&\quad +18xy^2z+17xyz^2+xz^3+17y^4+14y^3z+y^2z^2+5yz^3+7z^4.
\end{aligned}
$$

A computation shows that the first four quartics, $g_j(x,y,z)$, have 2 *automorphisms each, the next has* 4*, the next two have* 6*, the next three have* 8*, the next one has* 9*, and the final three have* 24 *each.*

We note that

$$T_7(19) = \frac{115}{36} = \frac{4}{2}+\frac{1}{4}+\frac{2}{6}+\frac{3}{8}+\frac{1}{9}+\frac{3}{24},$$

so these quartics account for all surfaces of maximal trace. This is the last case in which we intend to completely classify the del Pezzo surfaces of degree 2 of maximal trace. For $\mathbb{F}_{23}$ we first see a quartic $f_4(x,y,z)$ with trivial automorphism group such

that $w^2 = f_4(x, y, z)$ is the anti-canonical model of a del Pezzo surface of maximal trace.

Proposition 76. *There are at least* 19 *distinct isomorphism classes of degree* 2 *del Pezzo surfaces of maximal trace over* $\mathbb{F}_{23}$. *The equations* $w^2 = g_j(x, y, z)$ *where*

$$\begin{aligned} g_1(x,y,z) &= 18x^4 + 18x^3y + 11x^3z + 9x^2y^2 + 11x^2yz + 4x^2z^2 + 8xy^3 \\ &\quad +13xy^2z + 2xyz^2 + 7xz^3 + y^4 + 8y^2z^2 + 11yz^3 + 9z^4, \\ g_2(x,y,z) &= 4x^4 + x^3y + 12x^3z + 7x^2y^2 + 10x^2yz + 8x^2z^2 + 5xy^3 + 18xy^2z \\ &\quad +16xyz^2 + 10xz^3 + 8y^4 + 19y^3z + 4y^2z^2 + 5yz^3 + 13z^4, \end{aligned}$$

are anti-canonical models of surfaces of maximal trace. Each of these quartics has no non-trivial automorphisms.

Proof. Computation shows that $T_7(23) = \frac{461}{28} = 16 + \frac{13}{28}$. It takes at least 19 unit fractions to reach this sum. The two quartics in the proposition statement come from carrying out the process described above starting with a 7-tuple of points of $\mathbb{P}^2(\mathbb{F}_{23})$ in general position. □

We now turn to a different aspect of these counts. By studying congruence properties of the sextic polynomial in the numerator of $T_7(q)$ we can show that over certain fields $\mathbb{F}_q$ there must exist a maximal trace surface with anti-canonical model $w^2 = f_4(x, y, z)$, where $f_4(x, y, z)$ has an automorphism of given order.

Proposition 77. *Suppose that* q *is an odd prime power.*

(1) If $q \equiv 1, 2, 4 \pmod 7$ *then there exists a quartic* $f_4(x, y, z)$ *with an automorphism of order* 7 *such that* $w^2 = f_4(x, y, z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *of maximal trace.*

(2) *If* $q \equiv 1 \pmod 8$ *then there exists a quartic* $f_4(x,y,z)$ *with an automorphism group of order divisible by* 32 *such that* $w^2 = f_4(x,y,z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *of maximal trace.*

(3) *If* $q \equiv 0 \pmod 9$ *then there exists a quartic* $f_4(x,y,z)$ *with an automorphism group of order divisible by* 9 *such that* $w^2 = f_4(x,y,z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *of maximal trace.*

PROOF. We know that

$$T_7(q) = \frac{(q-7)(q-5)(q-3)(q^3-20q^2+119q-175)}{2^9 \cdot 3^4 \cdot 5 \cdot 7},$$

is equal to the sum of $|\mathrm{Aut}(C)|^{-1}$ taken over all non-isomorphic quartic curves C giving anti-canonical models of del Pezzo surfaces of maximal trace. We consider each of the prime powers dividing the denominator.

If there is a 7 in the denominator, for example, then one of these automorphism groups must have order divisible by 7. Since 7 is a prime, this in fact shows that there is an automorphism of order 7. Carefully considering congruence properties of values taken by the numerator of $T_7(q)$ completes the proof. □

The congruence condition on $T_7(q)$ allows $q \equiv 6 \pmod 9$ in the third statement, but this does not occur for q equal to a prime power. We could give conditions for smaller prime powers, for example congruence conditions on q that guarantee the existence of a quartic $f_4(x,y,z)$ with an automorphism of order 3 and giving the anti-canonical model of a maximal trace surface, but we do not pursue this here because such a condition will not determine the curve uniquely.

Corollary 78. *Suppose that* q *is a prime power.*

(1) *If* $q \equiv 1, 2, 4 \pmod 7$ *then there exists a homogeneous quartic* $f_4(x,y,z)$ *such that* $w^2 = f_4(x,y,z)$ *is the anti-canonical model of a del Pezzo surface*

of degree 2 *of maximal trace, and some lift of* $f_4(x, y, z)$ *is isomorphic to the Klein quartic curve.*

(2) If $q \equiv 1 \pmod 8$ *then* $w^2 = x^4 + y^4 + z^4$*, the Fermat quartic, gives the anti-canonical model of a del Pezzo surface of degree* 2 *of maximal trace.*

PROOF. The Klein quartic is the unique quartic curve over $\mathbb{C}$ with an automorphism group divisible by 7 and the Fermat quartic is the unique curve over $\mathbb{C}$ with an automorphism group of order divisible by 32. Therefore, a curve over $\mathbb{F}_q$ with an automorphism group of size divisible by 7 must have some lift isomorphic to the Klein quartic. We cannot write down a model of the Klein quartic that works in general here because the automorphisms are not all defined over $\mathbb{Q}$. For example, in one model of the Klein quartic we need -7 to be a square in $\mathbb{F}_q$ in order for all of the automorphisms to be defined over $\mathbb{F}_q$.

Similarly, a curve with the order of its automorphism group divisible by 32 must have a lift isomorphic to the Fermat quartic. All of the automorphisms of the Fermat quartic are defined over any field $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$. □

We note that for $q \equiv 5 \pmod 8$ the Fermat quartic appears to give the anti-canonical model $w^2 = x^4 + y^4 + z^4$ of a smooth surface of trace -5.

We can give similar kinds of results for quartics $f_4(x, y, z)$ such that $w^2 = f_4(x, y, z)$ is the anti-canonical model of del Pezzo surface with $q^2 + q + 1 + 6q$ $\mathbb{F}_q$-points. These surfaces are not maximal, but are near maximal. As we saw in the previous section, such a del Pezzo surface has a one-dimensional lattice generated by (-2)-curves.

Proposition 79. *Suppose that* q *is an odd prime power.*

(1) If $q \equiv 1 \pmod 4$ *there exists a quartic* $f_4(x, y, z)$ *with an automorphism of order* 5 *such that* $w^2 = f_4(x, y, z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *of trace* 6*.*

(2) If $q \equiv 1 \pmod 8$ *there exists a quartic* $f_4(x,y,z)$ *with an automorphism group of order divisible by* 16 *such that* $w^2 = f_4(x,y,z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *with trace* 6.

(3) If $q \equiv 1,2,4,8 \pmod 9$ *there exists a quartic* $f_4(x,y,z)$ *with an automorphism of order* 3 *such that* $w^2 = f_4(x,y,z)$ *is the anti-canonical model of a del Pezzo surface of degree* 2 *with trace* 6.

It will be useful for this proof and in the arguments that follow to define the analogue of $T_7(q)$ for trace 6 surfaces. Let

$$T_6(q) = \frac{(q-7)(q-5)(q-3)(q^3-20q^2+119q-175)}{2^8 \cdot 3^2 \cdot 5}.$$

This is $a_6 \frac{2}{|W(E_7)|}$ divided by $|\mathrm{GL}_3(\mathbb{F}_q)|$. Just as $T_7(q)$ is the sum of $|\mathrm{Aut}(C)|^{-1}$ over all non-isomorphic curves $f_4(x,y,z)$ with $w^2 = f_4(x,y,z)$ the anti-canonical model of a surface of maximal trace, $T_6(q)$ is this sum over all non-isomorphic curves C giving the anti-canonical model of a surface of trace 6.

Proof. We consider the prime factors that occur in the denominator of $T_6(q)$. Studying congruence properties of the quintic in the numerator shows that there is a factor of 5 in the denominator of $T_6(q)$ exactly when $q \equiv 1 \pmod 4$. Similarly, the denominator of $T_6(q)$ is divisible by 16 when $q \equiv 1 \pmod 8$, and is divisible by 3 when $q \equiv 1,2,4,8 \pmod 9$. □

We can also go through a similar analysis to the one used above for surfaces of maximal trace in order to study del Pezzo surfaces of near-maximal trace.

Proposition 80. *There is a unique del Pezzo surface of degree* 2 *of trace* 6 *over* $\mathbb{F}_9$. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_9)$, *its anti-canonical model is given by the homogeneous quartic* $w^2 = x^4 - y^4 + xyz^2$.

Proof. We compute $T_6(q) = \frac{1}{16}$. We found this quartic by starting with a 7-tuple of points in $\mathbb{P}^2(\mathbb{F}_q)$ in near general position and following the procedure to produce

an equation of the form $w^2 = f_4(x, y, z)$ described above. We get the quartic

$$\begin{aligned} f_4(x,y,z) &= 2ax^3y + (2a+1)x^2y^2 + 2x^2yz + (a+1)xy^3 + (2a+1)xy^2z \\ &\quad +(a+1)xyz^2 + (2a+2)y^3z + (a+1)y^2z^2 + x^4 + (a+1)y^4. \end{aligned}$$

We note that this curve has a unique singular point at $[x : y : z] = [0 : 0 : 1]$, since the z^4, xz^3 and yz^3 coefficients of this curve are 0. Some convenient changes of variables give us the form described in the statement.

It is no longer so straightforward to compute the size of the automorphism group of this curve. Magma does not return the size of the automorphism group of a singular curve, but of the normalization of the curve. In this case, the normalization has 48 automorphisms. However, with our nicer model it is possible to determine the automorphism group directly. We omit the details of this computation. □

We could continue this kind of analysis like we did above for maximal trace surfaces. We compute $T_6(11) = \frac{37}{60}$, so it is already clear that there is not a unique surface of trace 6. For $q \geq 13$ we see that $T_6(q) > 1$, so it is not possible for there to be a unique surface of trace 6.

Proposition 81. *The only finite field of odd characteristic for which there is a unique degree* 2 *del Pezzo surface of trace* 6 *is* $\mathbb{F}_9$.

We now turn to the values of q for which $\mathbb{F}_q$ does not have characteristic 2 or 3, and there are no del Pezzo surfaces of trace 6 or 7. These are $q = 5$ and $q = 7$.

Proposition 82. *There is a unique del Pezzo surface of degree* 2 *over* $\mathbb{F}_5$ *of trace* 5. *Up to automorphisms of* $\mathbb{P}^2(\mathbb{F}_5)$, *its anti-canonical model is* $w^2 = 2(x^4 + y^4 + z^4)$.

Proof. By Theorem 3 that there are 7750 equations of the form $w^2 = f_4(x, y, z)$ that are anti-canonical models of a del Pezzo surface of degree 2 of trace 5. It is not hard to verify that $f_4(x, y, z) = 2(x^4 + y^4 + z^4)$ gives one such surface and

that $f_4(x, y, z)$ is smooth. This curve has 96 automorphisms. Therefore, this curve contributes

$$\frac{|\mathrm{GL}_3(\mathbb{F}_5)|}{2 \cdot 96} = 7750$$

equations to the total count. □

The analogous count for surfaces of trace 5 over $\mathbb{F}_7$ is 10557540. Multiplying by $\frac{2}{|\mathrm{GL}_3(\mathbb{F}_7)|}$ gives $\frac{5}{8}$. Therefore, it is not possible that there is a unique smooth surface of trace 5 over $\mathbb{F}_7$.

4. Dual Code Coefficients from del Pezzo Surfaces of Degree 2

In this section we prove Theorems 63 and 64. The main idea is to determine the possible supports of a codeword of weight at most 10 of $C'^{\perp}_{2,4}$ and of $C^{c\perp}_{2,4}$ and then to find the number of codewords with given type of support by polynomial interpolation.

Recall that these codes have length $q^3 + q^2 + q$ corresponding to the nonsingular points of $\mathbb{P}(2, 1, 1, 1)$ with coordinates $[w : x : y : z]$. The standard affine representatives for $\mathbb{P}^2(\mathbb{F}_q)$ are the points $(1, a, b),\ (0, 1, a),\ (0, 0, 1)$, where $a, b \in \mathbb{F}_q$. We choose affine representatives for the nonsingular points of $\mathbb{P}(2, 1, 1, 1)$ given by (w, p) where $w \in \mathbb{F}_q$ and p is one of these standard affine representatives for $\mathbb{P}^2(\mathbb{F}_q)$. We think of each point p as having q values of w lying above it, giving q points (w, p) where $w \in \mathbb{F}_q$.

Suppose c is a codeword of $C'^{\perp}_{2,4}$ of weight k with with nonzero coordinates $a_1, \ldots, a_k$ corresponding to the points $\{(w_1, p_1), (w_2, p_2), \ldots, (w_k, p_k)\}$. These points are called the *support* of c. It will be important for us to consider the multiset given by the projection to $\mathbb{P}^2(\mathbb{F}_q)$, $\{p_1, \ldots, p_k\}$. This is a multiset that does not have to be a set because there can be distinct points (w_{i_1}, p_i) and (w_{i_2}, p_i) in the support of a codeword. We have

$$\alpha \sum_{i=1}^{k} a_i w_i^2 + \sum_{i=1}^{k} a_i f_4(p_i) = 0,$$

for all $\alpha \in \mathbb{F}_q$ and all homogeneous quartics $f_4(x, y, z)$. The only difference if c is a codeword of $C_{2,4}^{c\perp}$ is that we need only consider $\alpha = 0$. In this case, it is clear that once the multiset $\{p_1, \ldots p_k\}$ is fixed, we need only choose the values of w_i so that the points of the support are distinct.

It is only possible for this equality to hold for all homogeneous quartics of the form $\alpha w^2 - f_4(x, y, z)$ if both sums are zero. Suppose that this is not the case. Then there is a collection of points $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ and some collection of coefficients $a_1, \ldots, a_k$ for which the first sum $\alpha \sum_{i=1}^{k} a_i w_i^2$ is nonzero but

$$\alpha \sum_{i=1}^{k} a_i w_i^2 + \sum_{i=1}^{k} a_i f_4(p_i) = 0,$$

for all α and $f_4(x, y, z)$. Taking $\alpha = 0$ shows that this is not possible.

We consider the two sums separately. Let $\{p'_1, \ldots, p'_r\}$ be a maximal subset of distinct elements of $\{p_1, \ldots, p_k\}$. Then

$$\sum_{i=1}^{k} a_i f_4(p_i) = \sum_{j=1}^{r} a'_j f(p'_j) = 0,$$

where the a'_j are expressed as sums of the a_i. We focus on the subset of the a'_j that are nonzero. Call this set $\{b_1, \ldots, b_m\}$ and the corresponding points $\{p''_1, \ldots, p''_m\}$. This set defines a codeword of weight $m \leq r$ of $C_{2,4}^{\perp}$. The following result, Proposition 1 in [**19**], narrows down the possibilities for the set $\{p''_1, \ldots, p''_m\}$. This result is a step in the direction of the Cayley-Bacharach theorem.

Proposition 83. *Let $\Omega = \{p_1, \ldots, p_n\} \subset \mathbb{P}^2$ be any collection of $n \leq 2d + 2$ distinct points. The points of Ω fail to impose independent conditions on curves of degree d if and only if either $d + 2$ of the points of Ω are collinear or $n = 2d + 2$ and Ω is contained in a conic.*

We apply this to the case $d = 4$ and conclude that if $k \leq 10$ points fail to impose independent conditions on homogeneous quartics then either 6 points lie on a line or

$k = 10$ and these points are contained in a conic. In the case of 10 points, either 6 points lie on a line, all 10 points lie on a smooth conic, or the 10 points lie on a conic given as the union of two lines, exactly 5 points on each.

Corollary 84. *Either the set* $\{p''_1, \ldots, p''_m\}$ *consists of* m *collinear points, or* $m = 10$ *and this set is contained in a smooth conic, or is contained in two lines, exactly* 5 *points on each.*

PROOF. Suppose this is not the case. By the previous proposition, the set $\{p''_1, \ldots, p''_m\}$ contains 6 points on some line L and at least one point not on L. Consider such a configuration that has the minimal number of collinear points. We rearrange these points so that $\{p''_1, \ldots, p''_l\}$ is this set of collinear points. We see that $l \geq 6$. Without loss of generality suppose p''_m is not on L.

Consider any dual codeword with support $\{p''_1, \ldots, p''_m\}$ and nonzero coordinates $b_1, \ldots, b_m$ with each $b_i \neq 0$. For any 6 collinear points, for example $p''_1, \ldots, p''_6$, there is a dual codeword supported on these points with coefficients $c_1, \ldots, c_6$. Subtracting the appropriate scalar multiple of this codeword gives a dual codeword with the coordinate corresponding to p''_1 equal to 0. The support of this codeword is contained in $\{p''_2, \ldots, p''_m\}$. The number of collinear points of the support of this codeword is at most $l - 1$, contradicting the above assumption. □

This gives a complete description of the possible supports of a codeword of weight at most 10 of $C^{\perp}_{2,4}$. We now return to the dual codewords of weight at most 10 of $C'^{\perp}_{2,4}$ and $C^{c\perp}_{2,4}$.

Proposition 85. *Let* c *be a codeword of weight at most* 10 *of either* $C'^{\perp}_{2,4}$ *or* $C^{c\perp}_{2,4}$ *with support* $\{(w_1, p_1), \ldots, (w_k, p_k)\}$. *Let* $\{p'_1, \ldots, p'_r\}$ *be the underlying set of points* p_i.

(1) If $k \leq 9$ *then the set* $\{p'_1, \ldots, p'_r\}$ *either consists of at most four points, or is contained in a line together with one point not on the line.*

(2) If $k = 10$ and $r < 10$ then the set $\{p'_1, \ldots, p'_r\}$ either consists of at most five points, or is contained in a line together with two points not on the line.

(3) If $k = 10$ and $r = 10$ then the set $\{p'_1, \ldots, p'_{10}\}$ either consists of ten points on a line, ten points on a smooth conic, or ten points contained in two lines, exactly five points on each.

PROOF. Suppose c has nonzero coordinates $a_1, \ldots, a_k$ corresponding to the points of its support. For each $p'_i \in \{p'_1, \ldots, p'_r\}$ let a'_i be the sum of a_j for all points of the support (w_j, p_j) with $p_j = p'_i$. Let $\{b_1, \ldots, b_m\}$ be the multiset of a'_i that are nonzero and let $\{p''_1, \ldots, p''_m\}$ be the corresponding set of points. As above, the coordinates $\{b_1, \ldots, b_m\}$ determine an element of $C^{\perp}_{2,4}$ of weight m. The third statement follows directly from Corollary 84. That result also shows that if $m < 10$ then the points $\{p''_1, \ldots, p''_m\}$ are collinear.

Suppose p_j is such that $(w_{j_1}, p_j), \ldots, (w_{j_l}, p_j)$ are points of the support of c with nonzero coordinates $a_{j_1}, \ldots, a_{j_l}$. Then

$$\sum_{i=1}^{l} a_{j_i} f_4(p_j) = 0$$

implies that $\sum_{i=1}^{l} a_{j_i} = 0$. Therefore, $l \geq 2$. It is possible to have $l = 2$ since $af_4(p'_j) + (-a)f_4(p'_j) = 0$ for all $f_4(x, y, z)$. Therefore, the set $\{p'_1, \ldots, p'_r\}$ consists of $m \geq 6$ collinear points together with at most $\lfloor \frac{r-m}{2} \rfloor$ other points. □

This result classifies the sets $\{p'_1, \ldots, p'_r\}$ that occur for a dual codeword of weight at most 10. The next goal is to count the number of codewords that have a specific type of underlying set. For weight at most 7 it is not so difficult to give explicit formulas the number of codewords with each possible type of underlying set $\{p'_1, \ldots, p'_r\}$, but for weights $8, 9$, and 10 the counts become very intricate. We determine these counts by showing that for each weight $k \leq 10$ and each possible type of set $\{p'_1, \ldots, p'_r\}$, the number of codewords of $C'^{\perp}_{2,4}$ and of $C^{c\perp}_{2,4}$ of weight k with

this type of underlying set is given by a polynomial in q, with a single exception. The count for weight 10 codewords of $C'^{\perp}_{2,4}$ where $\{p'_1, \ldots, p'_r\}$ are 10 points on a line involves $\tau(q)$. We consider this case separately.

We recall the definition of a code restricted to a subset. For a code C over $\mathbb{F}_q^N$ and a set $\{i_1, \ldots, i_k\} \subseteq [1, N]$, the code C restricted to this set is the image of the map taking $c = (c_1, \ldots, c_N)$ to $c' \in \mathbb{F}_q^{N-k}$ where all of the coordinates except $c_{i_1}, \ldots, c_{i_k}$ are omitted. This map is not necessarily injective. In this case, C restricted to this set is actually a multiset of codewords.

Lemma 86. *Let C' denote either the code $C'_{2,4}$ or the code $C^c_{2,4}$. Let*

$$S := \{(w_1, p_1), \ldots, (w_k, p_k)\}$$

denote a subset of distinct points of $\mathbb{P}(2, 1, 1, 1)$. Let $C'|_S$ denote the code C' restricted to the coordinates corresponding to points of S. The number of codewords of $C'^{\perp}$ of weight r supported on S is given by the $X^{k-r}Y^r$ coefficient of

$$\frac{1}{|C'|} W_{C'|_S}(X + (q-1)Y, X - Y).$$

Proof. This is a straightforward application of the MacWilliams theorem and the definition of a dual code coefficient of a code that comes from evaluating polynomials. When the set S is small it is possible that codewords corresponding to distinct polynomials can be equal, that is, the kernel of the map taking a polynomial to an element of $\mathbb{F}_q^k$ is non-trivial. In this case the size of the kernel is cancelled by the appropriate factor of $|C'|^{-1}$. □

As an example, we determine the number of codewords of weight at most 10 of $C^{c\perp}_{2,4}$ supported on the q points (w, p_1), where p_1 is fixed and $w \in \mathbb{F}_q$. Such a codeword has underlying set $\{p'_1, \ldots, p'_r\} = \{p_1\}$ in the notation defined above. It is clear that there are no such codewords of weight 1.

Suppose that c is a codeword of weight 2 with support (w_1, p_1) and (w_2, p_1) and nonzero coordinates a_1 and a_2. By definition $w_1 \neq w_2$ and $a_1 f_4(p_1) + a_2 f_4(p_1) = 0$ for all homogeneous quartics $f_4(x, y, z)$. Therefore, $a_2 = -a_1$. This gives $q - 1$ such codewords. We check that this matches the computation from the previous lemma.

There are q^{15} homogeneous quartics $f_4(x, y, z)$ and q^{14} of them vanish at a given point p_1. This gives

$$W_{C'|_S}(X, Y) = q^{14}X^2 + (q^{15} - q^{14})Y^2.$$

Therefore

$$\begin{aligned} \frac{1}{q^{15}} W_{C'|_S}(X + (q-1)Y, X - Y) &= \frac{1}{q^2}\left(q(X + (q-1)Y)^2 + (q^2 - q)(X - Y)^2\right) \\ &= X^2 + (q-1)Y^2, \end{aligned}$$

for the set S consisting of these two chosen points.

We can similarly count the number of such codewords where w_1 and w_2 are allowed to vary. This multiplies the previous count by $\frac{q(q-1)}{2}$, which we could also see from the weight enumerator of the punctured code. We have

$$\begin{aligned} &\frac{1}{q^{15}} W_{C'|_S}(X + (q-1)Y, X - Y) = \frac{1}{q}\left((X + (q-1)Y)^q + (q-1)(X - Y)^q\right) \\ = \;& X^q + \frac{(q-1)^2 q}{2} X^{q-2}Y^2 + \frac{(q-1)^2(q-2)^2 q}{6} X^{q-3}Y^3 + O(Y^4). \end{aligned}$$

For a weight k codeword supported on points of the form (w, p_1) the k values of w_i can be chosen arbitrarily as long as they are distinct, and the nonzero coordinates a_i can be chosen arbitrarily as long as they sum to 0. It is clear that for all k the number of codewords of this type is a polynomial in q.

We now investigate the codewords supported on points of the form (w, p_1) of $C'^{\perp}_{2,4}$. A weight k codeword still comes from choosing the nonzero coordinates a_i that

sum to 0, but there is now the additional condition that $\sum_{i=1}^{k} a_i w_i^2 = 0$. We have $a_k = -(a_1 + \cdots + a_{k-1})$.

We first choose k distinct values $w_1, \ldots, w_k$. The goal is to count solutions to

$$a_1(w_1^2 - w_k^2) + a_2(w_2^2 - w_k^2) + \cdots + a_{k-1}(w_{k-1}^2 - w_k^2) = 0,$$

such that each a_i is nonzero. Since $w_j \neq w_k$ for $j \neq k$ the only way for $w_j^2 - w_k^2 = 0$ is for $w_j = -w_k$. We see that this can hold for at most one value of $j \in [1, k-1]$.

We consider two cases based on whether there is a term $w_j^2 - w_k^2 = 0$ for some $j < k$. We claim that in each case the number of solutions with each $a_i \neq 0$ is given by a polynomial in q. We prove this by induction on k. This holds for $k = 1$ where we note that all solutions correspond to the case where $w_1^2 - w_2^2 = 0$. Suppose this holds for all $k \leq m - 1$.

First suppose that there is some $j < m$ for which $w_j^2 - w_k^2 = 0$. Without loss of generality, suppose that $w_1^2 - w_k^2 = 0$. Then a_1 can be any nonzero element of $\mathbb{F}_q^*$ and

$$a_2(w_2^2 - w_m^2) + \cdots + a_{m-1}(w_{m-1}^2 - w_m^2) = 0,$$

where each $w_j^2 - w_m^2 \neq 0$. By induction, the number of such solutions $a_1, \ldots, a_{m-1}$ with each a_j nonzero is given by a polynomial in q.

We now consider the case where each $w_j^2 - w_k^2 \neq 0$. There are q^{k-2} solutions $a_1, \ldots, a_{k-1}$, but we only want to count the ones for which each $a_i \neq 0$. By letting $a_i' = a_i(w_i^2 - w_k^2)^{-1}$, we see that this does not depend on the choice of $w_1, \ldots, w_k$. We need only note that for each k, the number of solutions of $a_1 + \cdots + a_{k-1} = 0$ where each a_i is nonzero is given by a polynomial in q. We summarize this below.

Lemma 87. *For each $k \leq 10$, the number of codewords of weight k of $C_{2,4}'^{\perp}$ that are supported on points of the form (w, p_1) where $w \in \mathbb{F}_q$ and p_1 is fixed, is given by a polynomial in q.*

We can find these polynomials explicitly by Lagrange interpolation. We note that the number of codewords of weight k is bounded by q^{2k}, the number of possibilities for the nonzero coordinates $a_1, \ldots, a_k$ times the number of possibilities of the points $(w_1, p_1), \ldots, (w_k, p_1)$.

Corollary 88. *The contribution to the weight enumerator of $C'^{\perp}_{2,4}$ from codewords of weight at most 10 that are supported on points of the form (w, p_1) where $w \in \mathbb{F}_q$ and p_1 is fixed, is given by*

$$(q-1)^2 \sum_{j=2}^{10} \frac{A_j(q)}{j!} X^{q^3+q^2+q-j} Y^j,$$

where the $A_j(q)$ are given by:

$$\begin{aligned}
A_2(q) &= 1 \quad A_3(q) = (q-3)(q-2) \\
A_4(q) &= (q-3)(q-2)\left(q^2 - 3\,q + 6\right) \\
A_5(q) &= (q-4)(q-3)(q-2)\left(q^3 - 4\,q^2 + 6\,q - 10\right) \\
A_6(q) &= (q-5)(q-4)(q-3)(q-2)\left(q^4 - 5\,q^3 + 10\,q^2 - 10\,q + 15\right) \\
A_7(q) &= (q-6)(q-5)(q-4)(q-3)(q-2)\left(q^5 - 6\,q^4 + 15\,q^3 - 20\,q^2 + 15\,q - 21\right) \\
A_8(q) &= (q-7)\,(q-6)(q-5)\,(q-4)\,(q-3)(q-2)\Big(q^6 - 7\,q^5 + 21\,q^4 - 35\,q^3 \\
&\qquad +35\,q^2 - 21\,q + 28\Big) \\
A_9(q) &= (q-8)(q-7)(q-6)(q-5)(q-4)(q-3)\,(q-2) \\
&\times \left(q^7 - 8\,q^6 + 28\,q^5 - 56\,q^4 + 70\,q^3 - 56\,q^2 + 28\,q - 36\right) \\
A_{10}(q) &= (q-9)(q-8)(q-7)(q-6)(q-5)(q-4)(q-3)(q-2) \\
&\times \left(q^8 - 9\,q^7 + 36\,q^6 - 84\,q^5 + 126\,q^4 - 126\,q^3 + 84\,q^2 - 36\,q + 45\right).
\end{aligned}$$

Allowing different choices of p_1 multiplies this expression by $q^2 + q + 1$.

It is easy to give a similar result for $C_{2,4}^{c\perp}$ but we do not exhibit it here.

The same argument gives a similar statement for dual codewords c of either $C_{2,4}^{\prime\perp}$ or $C_{2,4}^{c\perp}$ of weight at most 10 supported on the $5q$ points of the form $(w, p_1), \ldots, (w, p_5)$, where each p_i is fixed and $w \in \mathbb{F}_q$ is allowed to vary. Such a codeword of weight $k \leq 10$ with nonzero coordinates $a_1, \ldots, a_k$ satisfies

$$\sum_{i=1}^{k} a_i f_4(p_i) = 0,$$

for all homogeneous quartics $f_4(x, y, z)$. By Corollary 84, for each $j \in [1, 5]$ the sum of the a_i taken over all i such that $p_i = p_j$ is zero. For $C_{2,4}^{\prime\perp}$ the inclusion-exclusion needed to determine these counts exactly becomes complicated, but the arguments given above show the following. We note that there are $\binom{q^2+q+1}{k}$ ways to choose k points in $\mathbb{P}^2(\mathbb{F}_q)$, and this is a polynomial in q of degree $2k$.

Proposition 89. *Let C' denote the code $C_{2,4}'$ or $C_{2,4}^c$. The number of codewords of $C'^{\perp}$ of weight $k \leq 10$ with support $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ such that the multiset $\{p_1, \ldots, p_{10}\}$ contains at most 5 distinct points is given by a polynomial in q of degree at most $4k$.*

Using this result and inclusion-exclusion it is possible to find for each $k \leq 10$ and for each j satisfying $1 \leq j \leq 5$ the number of such codewords of weight k such that $\{p_1, \ldots, p_{10}\}$ contains exactly j distinct points. For example, the number of weight 10 codewords of $C_{2,4}^{\prime\perp}$ such that the set $\{p_1, \ldots, p_{10}\}$ contains exactly 5 distinct points is

$$\binom{q^2+q+1}{5} \frac{(q-1)^{10} q^4}{32}.$$

The initial factor comes from choosing 5 points in $\mathbb{P}^2(\mathbb{F}_q)$ and the rest comes from counting codewords supported on 5 chosen points.

We next turn to one of the more complicated types of support described in Corollary 84, namely 10 points on a smooth conic.

Proposition 90. *The number of codewords of $C_{2,4}^{\perp}$ of weight 10 supported on a given smooth conic is $(q-1)\binom{q+1}{10}$.*

PROOF. We claim that given any 10 points on a smooth conic there is a unique dual codeword supported on these points up to scalar multiplication. The count is given by $q-1$ times the number of collections of 10 points on a smooth conic. By Bézout's theorem a quartic intersecting a given conic at 9 points $p_1, \ldots, p_9$ must contain that conic. Given such a collection and any additional point of the conic p_{10} we can express

$$f_4(p_{10}) = \sum_{i=1}^{9} a_i f_4(p_i),$$

for a unique linear combination $a_1, \ldots, a_9$, completing the proof. □

Lemma 91. *Suppose that c is a weight 10 codeword of $C_{2,4}^{\perp}$ supported on a smooth conic. Then the product of the nonzero coordinates of c is -1 times a nonzero square in $\mathbb{F}_q^*$.*

We recall that a diagonal quadric in $\mathbb{P}^{m-1}(\mathbb{F}_q)$ defines a plus quadric if the product of the diagonal coefficients takes the same value that $(-1)^{\frac{m}{2}}$ does under the quadratic character on $\mathbb{F}_q^*$. This follows directly from taking the product of the relevant Gauss sums. This lemma gives exactly the condition required for a diagonal form in 10 variables with these coefficients to define a smooth plus quadric in $\mathbb{P}^9(\mathbb{F}_q)$.

PROOF. A smooth conic has $q+1$ points so if $q+1 < 10$ there is nothing to prove. For $q = 9$ we can verify this proposition directly by looking at the dual of the code of quartics restricted to a particular smooth conic, say $x^2+y^2+z^2$, using the fact that $\mathrm{PGL}_3(\mathbb{F}_q)$ acts transitively on smooth conics. There is a unique codeword supported on these ten points up to scalar multiplication. We can explicitly compute the linear

relation satisfied by these ten points

$$\sum_{i=1}^{10} a_i f_4(p_i) = 0,$$

for all quartic polynomials $f_4(x, y, z)$. In each case, the product of the a_i is a square.

Now suppose that $q > 9$. A smooth conic is given by a quadratic embedding $[x^2 : xy : y^2]$ of $\mathbb{P}^1(\mathbb{F}_q)$ after a change of coordinates. A homogeneous quartic restricted to this conic is just a homogeneous polynomial of degree 8 in x and y, the coordinates of the original $\mathbb{P}^1(\mathbb{F}_q)$. Therefore, 10 points on this conic fail to impose independent conditions on these quartics. The statement to be proven is equivalent to showing that the product of the nonzero coordinates of a weight 10 codeword in the dual of the code of homogeneous degree 8 polynomials on $\mathbb{P}^1(\mathbb{F}_q)$ takes the same value as -1 under the quadratic character.

Given 10 points $p_1, \ldots, p_{10}$ on $\mathbb{P}^1(\mathbb{F}_q)$ we apply an automorphism of $\mathbb{P}^1(\mathbb{F}_q)$ so that $[1 : 0]$ is not one of these points. We dehomogenize and suppose that these points are represented by $x_1, \ldots, x_{10}$ in $\mathbb{F}_q$. We define

$$Q(x) = \prod_{i=1}^{10}(x - x_i), \text{ and } R_{jk}(x) = \frac{Q(x)}{(x - x_j)(x - x_k)},$$

for each pair j, k satisfying $1 \leq j < k \leq 10$. There is a linear relation among these points

$$c_1 f(x_1) + \cdots + c_{10} f(x_{10}) = 0,$$

for all $f(x)$ of degree at most 9. Let $f(x) = R_{jk}(x)$. Note that $R_{jk}(x_k) \neq 0$. Then

$$c_j R_{jk}(x_j) + c_k R_{jk}(x_k) = 0, \quad \text{and so} \quad \frac{c_j}{c_k} = (-1)\,\frac{R_{jk}(x_j)}{R_{jk}(x_k)}.$$

We have

$$\prod_{j=2}^{10} \frac{c_1}{c_j} = \frac{c_1^9}{c_2 c_3 \cdots c_{10}} = (-1)^9 \prod_{i=2}^{10} \frac{R_{1i}(x_1)}{R_{1i}(x_i)}.$$

Multiplying the left hand side by $(c_2 \cdots c_{10})^2$ we see that it is a square times the product $c_1 c_2 \cdots c_{10}$. The right hand side is

$$(-1)\,\frac{\prod_{i=2}^{10}(x_i - x_1)^8}{\prod_{2\le i<j\le 10}(x_i - x_j)(x_j - x_i)}.$$

This is -1 times $(-1)^{\binom{9}{2}} = 1$ times a square, completing the proof. □

Proposition 92. *The number of weight* 10 *codewords of* $C'^{\perp}_{2,4}$ *that have support* $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ *such that* $p_1, \ldots, p_{10}$ *are* 10 *distinct points on a smooth conic in* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$(q-1)(q^5 - q^2)\binom{q+1}{10}\left(q^9 + (q-1)q^4\right).$$

The number of weight 10 *codewords of* $C^{c\perp}_{2,4}$ *with support* $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ *such that* $p_1, \ldots, p_{10}$ *are* 10 *distinct points on a smooth conic in* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$(q-1)(q^5 - q^2)\binom{q+1}{10}q^{10}.$$

Proof. The number of smooth conics in $\mathbb{P}^2(\mathbb{F}_q)$ is $q^5 - q^2$. The number of possibilities for $p_1, \ldots, p_{10}$ lying on a particular smooth conic is given by Proposition 90.

By the previous lemma, if c is a weight 10 codeword of $C'^{\perp}_{2,4}$ that has support $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ with nonzero coordinates $a_1, \ldots, a_{10}$ and $p_1, \ldots, p_{10}$ satisfying the conditions of this proposition, then

$$\sum_{i=1}^{10} a_i w_i^2 = 0.$$

Since $\prod_{i=1}^{10} a_i$ is -1 times a nonzero square, $\sum_{i=1}^{10} a_i x_i^2$ defines a plus quadric in $\mathbb{P}^9(\mathbb{F}_q)$. Such a quadric has $\frac{q^9-1}{q-1} + q^4$ $\mathbb{F}_q$-rational points. Taking scalar multiples of these projective points and adding in the possibility $(w_1, \ldots, w_{10}) = (0, \ldots, 0)$ gives $q^9 + (q-1)q^4$ possibilities for $(w_1, \ldots, w_{10})$.

If c is a weight 10 codeword of $C_{2,4}^{c\perp}$ satisfying the conditions of this proposition then there are q^{10} possibilities for $(w_1, \ldots, w_{10})$. $\square$

Now suppose that c is a codeword of weight $k \leq 10$ of $C_{2,4}'^{\perp}$ or of $C_{2,4}^{c\perp}$ that has support $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ and nonzero coordinates $a_1, \ldots, a_k$. Consider the multiset $\{p_1, \ldots, p_k\}$ and the underlying set $\{p_1', \ldots, p_r'\}$. Let a_j' be the sum of the a_i such that $p_i = p_j'$. As we discussed above, some of the r values $a_1', \ldots, a_r'$ may be zero. Let $b_1, \ldots, b_m$ be the set that are nonzero. We have analyzed codewords with $p_1, \ldots, p_{10}$ lying on a smooth conic and codewords where each $a_i' = 0$.

We now consider the case where the points $\{p_1', \ldots, p_r'\}$ are collinear. We then consider the case where we have a set of collinear points, and at most two other points. Let L denote a fixed line in $\mathbb{P}^2(\mathbb{F}_q)$. For concreteness, we may suppose that L is given by $z = 0$. Suppose we consider the code $C_{2,4}'$ punctured on all coordinates except those corresponding to points (w, p), where $w \in \mathbb{F}_q$ and $p \in L$. This punctured code has length $q^2 + q$.

In Chapter 3 we studied the quadratic residue weight enumerator of the code $C_{1,4}$ with codewords corresponding to homogeneous quartics $f_4(x, y)$ on $\mathbb{P}^1(\mathbb{F}_q)$. We determined $\mathrm{QR}_{C_{1,4}}(X, Y, Z)$ and studied the specialization $\mathrm{QR}_{C_{1,4}}(X, X^2, 1)$. This latter polynomial tells us the distribution of point counts for the q^5 homogeneous quartics on $\mathbb{P}(2, 1, 1)$ of the form $w^2 - f_4(x, y)$. This is the $\alpha = 1$ part of the weight enumerator of the six dimensional code of homogeneous quartics in the weighted projective space $\mathbb{P}(2, 1, 1)$ given by equations of the form $\alpha w^2 - f_4(x, y)$. This is very similar to the setup of the current problem. It is easy to write down the weight enumerator of the 5-dimensional subcode given by $\alpha = 0$, and we see that for each $k \leq 10$ the number of dual codewords of weight k is given by a polynomial in q.

We computed a homogenized version of the polynomial $\mathrm{QR}_{C_{1,4}}(X, X^2, 1)$ and then applied the classical MacWilliams theorem to it. Proposition 54 connected this weight enumerator to the weight enumerator coming from the q^5 homogeneous

quartics $w^2 = f_4(x, y)$ on $\mathbb{P}(2, 1, 1)$. We note that the preimage in $\mathbb{P}(2, 1, 1, 1)$ of a line in the $[x : y : z]$ projective plane is a copy of $\mathbb{P}(2, 1, 1)$. After applying the MacWilliams transformation to this weight enumerator of these q^5 codewords we saw that the Y^{10} coefficient was a polynomial in q plus a polynomial in q times $\tau(q)$. For each k satisfying $0 \leq k \leq 9$, the Y^k coefficient is given by a polynomial in q.

Proposition 93. *The number of codewords $c \in C'^{\perp}_{2,4}$ of weight 10 with support $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ such that $p_1, \ldots, p_{10}$ are distinct points on a line is equal to $P_1(q) + P_2(q) \cdot \tau(q)$, where $P_1(q), P_2(q)$ are polynomials in q of degree at most 32.*

Proof. This follows directly from Theorem 52 since the code coming from varieties of the form $w^2 - f_4(x, y, z)$ restricted to a line is equivalent to the code coming from varieties of the form $w^2 - f_4(x, y)$. To make this more concrete, since $\mathrm{PGL}_3(\mathbb{F}_q)$ acts transitively on lines we can choose the particular line given by $z = 0$.

The bound on the degree comes from the fact that there are at most $(q + 1)^{10}q^{10}$ possibilities of $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ for a given line, at most $(q - 1)^{10}$ choices of nonzero coordinates $(a_1, \ldots, a_{10})$, and exactly $q^2 + q + 1$ lines. □

Proposition 94. *For each $k \leq 10$, the number of codewords $c \in C^{c\perp}_{2,4}$ of weight k with support $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ such that $p_1, \ldots, p_k$ are contained in a line is given by a polynomial in q of degree at most $3k + 2$.*

For each $k \leq 9$, the number of codewords $c \in C'^{\perp}_{2,4}$ of weight k with support $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ such that $p_1, \ldots, p_k$ are points in a line is given by a polynomial in q of degree at most $3k + 2$.

Proof. For the degree statement we note that there are at most $(q + 1)^k q^k$ possibilities of $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ for a given line, at most $(q - 1)^k$ choices of nonzero coordinates $(a_1, \ldots, a_k)$, and exactly q^2+q+1 lines. The rest of the statement follows from the discussion above. □

As a corollary we state the contribution to the weight enumerator of $C'^{\perp}_{2,4}$ from codewords of this type. We found this expression by computing the weight enumerator of $C'_{2,4}$ restricted to the line $z = 0$ for many small values of q, applying the MacWilliams theorem, and interpolating.

Corollary 95. *The contribution to* $W_{C'^{\perp}_{2,4}}(X, Y)$ *from codewords that have support* $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ *such that* $p_1, \ldots, p_k$ *are contained in a line is given by*

$$(q-1)^2(q+1)(q^2+q+1)\sum_{j=2}^{10}\frac{A_j(q)}{j!}X^{q^3+q^2+q-j}Y^j,$$

where the $A_j(q)$ *are:*

$$\begin{aligned}
A_2(q) &= 1, \quad A_3(q) = (q-3)(q-2)\\
A_4(q) &= (\,q^4 - 14\,q^3 + 30\,q^2 - 48\,q + 36)\\
A_5(q) &= (q-2)\big(11\,q^5 - 51\,q^4 + 96\,q^3 - 120\,q^2 + 142\,q - 120\big)\\
A_6(q) &= \Big(q^9 + 32\,q^8 - 317\,q^7 + 1292\,q^6 - 2979\,q^5 + 4390\,q^4 - 4646\,q^3 + 4195\,q^2 - 3510\,q + 1800\Big)\\
A_7(q) &= (q-2)\Big(q^{11} + 3\,q^{10} + 71\,q^9 - 1059\,q^8 + 5215\,q^7\\
&\quad -13904\,q^6 + 23381\,q^5 - 26593\,q^4 + 22530\,q^3 - 16467\,q^2 + 12582\,q - 7560\Big)\\
A_8(q) &= (q-2)\Big(q^{14} + 3\,q^{13} - 28\,q^{12} + 212\,q^{11} - 3633\,q^{10} + 27323\,q^9 - 109335\,q^8 + 271198\,q^7\\
&\quad -449398\,q^6 + 521763\,q^5 - 442785\,q^4 + 301189\,q^3 - 190022\,q^2 + 130032\,q - 70560\Big)\\
A_9(q) &= (q-2)\Big(q^{17} + 3\,q^{16} - 37\,q^{15} - 81\,q^{14} + 1477\,q^{13} - 14561\,q^{12} + 124477\,q^{11} - 681919\,q^{10}\\
&\quad +2401876\,q^9 - 5733040\,q^8 + 9629370\,q^7 - 11636558\,q^6 + 10325912\,q^5 - 6983436\,q^4 + 4000252\,q^3\\
&\quad -2277288\,q^2 + 1448352\,q - 725760\Big)\\
A_{10}(q) &= \big(q^{21} + q^{20} - 53\,q^{19} - 8\,q^{18} + 1258\,q^{17} + 1619\,q^{16} - 78694\,q^{15} + 744136\,q^{14} - 5008985\,q^{13}\\
&\quad +24916147\,q^{12} - 90514598\,q^{11} + 242287029\,q^{10} - 484799964\,q^9 + 732875889\,q^8 - 841222633\,q^7\\
&\quad +735105906\,q^6 - 494759040\,q^5 + 269674245\,q^4 - 136112652\,q^3 + 74629836\,q^2 - 42930000\,q + 16329600\big)\\
&\quad -(q-1)q^5\tau(q).
\end{aligned}$$

The term involving $\tau(q)$ exactly cancels with the term involving $\tau(q)$ coming from $W^{G1}_{C'_{2,4}}(X+(q-1)Y, X-Y)$. We can easily give a similar result for the contribution to the weight enumerator of $C^{c\perp}_{2,4}$, but do not write it here.

For small weight codewords we can explain the individual terms contributing to this sum. For weight $8, 9$, and 10 there are so many possibilities to consider that it would be very difficult to write down this polynomial without some sort of interpolation argument.

For example, we saw above that every codeword of weight 2 that has support $\{(w_1, p), (w_2, p)\}$ has nonzero coordinates a and $-a$. There are $q+1$ choices for p and must choose $w_1 \neq w_2$ satisfying $aw_1^2 - aw_2^2 = 0$. Since $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$, we conclude $w_1 + w_2 = 0$. This gives $(q+1)\frac{(q-1)^2}{2}$ such codewords.

A codeword of weight 3 has $\{(w_1, p), (w_2, p), (w_3, p)\}$ with nonzero coordinates $a, b, -(a+b)$. There are $q+1$ choices of p and $(q-1)(q-2)$ choices of a and b. We must have $aw_1^2 + bw_2^2 - (a+b)w_3^2 = 0$, where the w_i are distinct. The equation $ax_1^2 + bx_2^2 - (a+b)x_3^2$ defines a smooth conic in $\mathbb{P}^2(\mathbb{F}_q)$, so it has $q+1$ rational points. There are 4 additional points that we do not want to count because of the constraint that the w_i are distinct. These are the affine representatives of the projective points: $\{[1:1:1], [1:1:-1], [1:-1:1], [-1:1:1]\}$. This gives $\frac{(q-1)(q-3)}{6}$ choices for the set $\{w_1, w_2, w_3\}$, explaining the Y^3 coefficient.

For the Y^4 coefficient the support can either be $\{(w_1, p), (w_2, p), (w_3, p), (w_4, p)\}$ for some point p with the w_i distinct, or can be $\{(w_1, p_1), (w_2, p_1), (w_3, p_2), (w_4, p_2)\}$ for some choice of $p_1 \neq p_2$ where $w_1 \neq w_2$ and $w_3 \neq w_4$. We can determine the number of codewords of each type and add them to get this term. We can do something very similar for the weight 5 coefficient since there are still at most two distinct values of p that occur.

For weight 6, things become a little more complicated. We consider the set of (w_i, p_i) where $1 \leq i \leq 6$. We can count codewords where exactly $1, 2$, or 3 distinct

values of p_i occur as above. However, it is possible now that all of the p_i are distinct. In this case,

$$\sum_{i=1}^{6} a_i f_4(p_i) = 0 \text{ for all } f_4(x,y),$$

so these six points and the nonzero coordinates a_i define a weight 6 codeword of $C_{1,4}^{\perp}$. We have seen that any 6 points support a unique such codeword up to scalar multiplication. Moreover, for such a codeword the product of the a_i is a nonzero square if $q \equiv 1 \pmod 4$, and is a non-square if $q \equiv 3 \pmod 4$. Therefore $\sum_{i=1}^{6} a_i x_i^2$ defines a plus quadric in $\mathbb{P}^5(\mathbb{F}_q)$, which has exactly $q^4 + q^3 + 2q^2 + q + 1$ $\mathbb{F}_q$-points. Taking scalar multiples and adding in the case where $(w_1, \ldots, w_6) = (0, \ldots, 0)$ gives $q^5 + (q-1)q^2$. The number of codewords of this type is

$$(q-1)\binom{q+1}{6}(q^5 + (q-1)q^2).$$

Adding these terms gives the weight 6 coefficient.

The weight 7 coefficient is the last case we analyze in complete detail. We determine the counts where $1, 2$, or 3 distinct values of p_i occur as above. We determine the number of codewords such that the 7 values of p_i are distinct using the number of weight 7 codewords of $C_{1,4}^{\perp}$. The resulting quadric in $\mathbb{P}^6(\mathbb{F}_q)$ given by $\sum_{i=1}^{7} a_i x_i^2$ is smooth, and all such quadrics have the same number of rational points.

The more complicated situation in where exactly 6 distinct points p_i occur among these 7 points and one occurs twice. For this repeated point there are two nonzero coordinates a, b such that $a + b \neq 0$. Given a choice of 6 points there is a unique codeword of $C_{1,4}^{\perp}$ supported on them. There are $\frac{(q-1)(q-2)}{2}$ total choices of this pair $\{a, b\}$. When considering the possibilities for $(w_1, \ldots, w_7)$ that lie on a smooth quadric in $\mathbb{P}^6(\mathbb{F}_q)$ we must subtract the number of points for which the two w-values above the point p occurring twice are equal. Restricting a smooth quadric to a hyperplane $x_i = x_j$ gives a smooth quadric in $\mathbb{P}^5(\mathbb{F}_q)$. Since the coefficients attached to the 6 distinct points that occur define a weight 6 codeword of $C_{1,4}^{\perp}$, this is a plus quadric

in $\mathbb{P}^5(\mathbb{F}_q)$. Taking scalar multiples gives an extra factor of $q-1$. Therefore, the total number of codewords of this form is

$$6\binom{q+1}{6}\frac{(q-1)(q-2)}{2}(q-1)^2((q^5+q^4+q^3+q^2+q+1)-(q^4+q^3+2q^2+q+1)).$$

Adding these terms gives the weight 7 term. We will not explain the weight $8, 9$, and 10 coefficients in detail, but use the fact that the remaining terms are polynomials in q to find them by interpolation. We checked these calculations well past the bound on the degree of the resulting polynomials in order to get a check on the consistency of the output.

We now turn to the next possibility for the support of a codeword of $C'^{\perp}_{2,4}$ or $C^{c\perp}_{2,4}$ of weight $k \leq 10$. Suppose that such a codeword has support $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ such that $\{p_1, \ldots p_k\}$ is contained in a line together with two points, and has nonzero coordinates $a_1, \ldots, a_k$. Let $\{p'_1, \ldots, p'_r\}$ be the distinct values of p_i that occur. For each i satisfying $1 \leq i \leq r$ let a'_i be the sum of the a_j corresponding to points of the support (w_j, p_j) satisfying $p_j = p'_i$. Consider the set $\{b_1, \ldots, b_m\}$ of these a'_i that are nonzero, and the corresponding set of points $\{p''_1, \ldots, p''_m\}$. We see that this set of p''_i must be contained in a line. In the case where this set is empty, it is easy to count codewords of this type using the techniques described above. When this set is not empty, the nonzero coordinates b_i and the corresponding points give a weight m codeword of $C^{\perp}_{1,4}$, so $6 \leq m \leq 10$.

We have already analyzed the case where the set $\{p_1, \ldots, p_k\}$ is contained in a line L. The only interesting case left is where this does not occur, when some elements of this multiset of k points are equal to the two chosen points not lying on L. Let p' be one of these points not lying on L. In order for this c to give a dual codeword, the sum of the nonzero coefficients for points (w, p) in the support of c with $p = p'$ must be equal to zero. Therefore, we need only investigate a few new types of possible supports of codewords.

We describe these codewords by describing the multiset $\{p_1, \ldots, p_k\}$. The only weight 8 codewords of this type have 6 distinct points on a line, and one point off the line with two w-values above it. For weight 9 there are a few possibilities. There can be 7 distinct points on the line and one point off the line that occurs twice. There can also be 6 points on the line, one occurring twice, and a point off the line that also occurs twice. Finally, there can be 6 points on the line each occurring once, and one points off the line occurring three times.

For weight 10, we can have 6 points on the line each occurring once, and one point off the line occurring four times. We can have 6 points on the line each occurring once, and two distinct points off the line, each occurring twice. We can have 6 points on the line, exactly one occurring twice, and one point off the line occurring three times. We can have 6 points on the line, exactly two occurring twice, and one point off the line occurring twice. We can have 6 points on the line, exactly one occurring three times, and one point off the line occurring twice. We can have 7 distinct points on the line each occurring once, and one point off the line occurring three times. We can have 7 distinct points on the line exactly one occurring twice, and one point off the line occurring twice. We can have 8 distinct points on the line each occurring once, and one point off the line occurring twice.

Counting each such configuration is tedious, but the arguments given earlier in this section imply the following. Again, this result is related to the analogous result for $\mathbb{P}(2, 1, 1)$, Proposition 54.

Proposition 96. *Let C' denote either the code $C'_{2,4}$ or $C^c_{2,4}$. For each $k \in [8, 10]$, the number of weight k codewords of $C'^{\perp}$ with support $\{(w_1, p_1), \ldots, (w_k, p_k)\}$ such that the underlying set $\{p'_1, \ldots, p'_r\}$ of the multiset $\{p_1, \ldots, p_k\}$ is not contained in a line but is contained in a line together with two points, is given by a polynomial in q.*

We go through a particular example in detail. Similar techniques can be used to determine the counts for the other cases.

Suppose $c \in C'^{\perp}_{2,4}$ has support $\{(w_1, p_1), \ldots, (w_8, p_8)\}$ with coefficients $a_1, \ldots, a_8$ and that the multiset $\{p_1, \ldots, p_8\}$ consists of 7 distinct points. Suppose that $p_1, \ldots, p_6$ lie on a line and $p_7 = p_8$ is a point not on this line. So, $w_7 \neq w_8$. Since $a_1, \ldots, a_6$ gives a codeword of $C'^{\perp}_{2,4}$ of weight 6, the product of these coordinates is -1 times a nonzero square in $\mathbb{F}_q^*$ and $\sum_{i=1}^{6} a_i x_i^2$ defines a plus quadric in $\mathbb{P}^5(\mathbb{F}_q)$. Therefore,

$$a_7 w_7^2 - a_7 w_8^2 + \sum_{i=1}^{6} a_i w_i^2$$

defines a plus quadric in $\mathbb{P}^7(\mathbb{F}_q)$ since the product of the coordinates is a nonzero square in $\mathbb{F}_q^*$ and $(-1)^{\frac{7+1}{2}} = 1$. Such a plus quadric has $\sum_{i=0}^{6} q_i + q^3$ points. Multiplying by $q-1$ to account for scalar multiples and adding 1 for the solution $(0, \ldots, 0)$ gives $q^7 + (q-1)q^3$ solutions.

However, we must take into account the additional constraint that $w_7 \neq w_8$. We count the number of solutions that violate this condition. We see that $(w_1, \ldots, w_6)$ must satisfy

$$\sum_{i=1}^{6} a_i w_i^2 = 0,$$

the equation of a plus quadric in $\mathbb{P}^5(\mathbb{F}_q)$. Multiplying by $q-1$ for scalar multiples and by q to account for the value of w_7 and then adding in the solutions where $(w_1, \ldots, w_6) = (0, \ldots 0)$ gives

$$q + q(q-1)(q^4 + q^3 + 2q^2 + q + 1) = q^6 + q^3(q-1)$$

solutions. Subtracting gives $q^7 - q^6$ total possibilities for $(w_1, \ldots, w_8)$. We multiply this by $(q-1)\binom{q+1}{6}$, the number of choices of $a_1, \ldots, a_6$ and $p_1, \ldots, p_6$, and by q^2+q+1 to account for the number of choices of lines. We also have q^2 choices of p_7 not on that line. In total this gives

$$(q^2+q+1)q^2(q-1)\binom{q+1}{6}\frac{q-1}{2}(q^7 - q^6)$$

total dual codewords of weight 8 with support of this type. We could perform a similar type of analysis for other possible supports, but it is enough for our purposes to know that these counts are given by polynomials and then interpolate.

We now consider the final possibility for the support of a codeword.

Proposition 97. *Let $c \in C_{2,4}^{\perp}$ be a codeword of weight* 10 *with support consisting of exactly* 5 *points on each of two lines.*

The number of such codewords is

$$(q-1)(q^2+q+1)\frac{(q+1)q}{2}\binom{q}{5}^2.$$

Proof. The argument of Proposition 90 shows that any 10 points of a conic fail to impose dependent conditions on quartics, but we also know that if there is no subset of 6 collinear points then any subset of 9 of these points does impose independent conditions. Therefore we need only count the number of collections of 5 points on each of two lines.

We first choose the point of intersection of these lines and then note that there are $\frac{(q+1)q}{2}$ pairs of lines intersecting at this point. For each of these two lines there are $\binom{q}{5}$ ways to choose 5 points not including the intersection point. Taking scalar multiples gives an extra factor of $q-1$. This completes the count. □

Lemma 98. *If c is a weight* 10 *codeword of $C_{2,4}^{\perp}$ supported on the union of two lines then the product of the nonzero coordinates of c is -1 times a square in $\mathbb{F}_q^*$.*

Proof. We let $\{p_1, \ldots, p_5\}$ be the five points on the first line and $\{q_1, \ldots, q_5\}$ be the points of the second line. Let p' be the point of intersection of these two lines. We note that there is exactly one codeword supported on the points $p_1, \ldots, p_5, p'$ up to scalar multiplication, and exactly one supported on $q_1, \ldots, q_5, p'$ up to scalar multiplication. Taking the appropriate scalar multiples so that the coefficients of p' match, the difference gives a dual codeword of weight 10 supported on $p_1, \ldots, p_5, q_1, \ldots, q_5$.

Taking all possible pairs of lines and collections of 5 points on each line satisfying these conditions along with a choice of scalar multiple produces exactly the number of codewords given in the previous proposition.

The product of the coefficients of the codeword c_1 with support $p_1, \ldots, p_5, p'$ is always -1 times a nonzero square in $\mathbb{F}_q^*$, independent of the scalar multiple that we take, and the same statement is true of the codeword c_2 with support $q_1, \ldots, q_5, q'$. Now without loss of generality suppose the scalar multiples are chosen so that the p' coefficient of each is 1. The product of the coefficients of c_1 and c_2 is a square. The weight 10 codeword that we get from the difference $c_1 - c_2$ is equal to the product of the coefficients of $p_1, \ldots, p_5$ in c_1 times $(-1)^5$ times the product of the coefficients of $q_1, \ldots, q_5$ in c_2. This is a square divided by -1, since we have omitted the coefficient of p' in both c_1 and $-c_2$. □

This lemma shows that such a codeword of weight 10 with nonzero coefficients $a_1, \ldots, a_{10}$ leads to a plus quadric in $\mathbb{P}^9(\mathbb{F}_q)$ given by $\sum_{i=1}^{10} a_i x_i^2 = 0$.

Proposition 99. *The number of weight* 10 *codewords of* $C'^{\perp}_{2,4}$ *that have support* $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ *such that* $\{p_1, \ldots, p_5\}$ *are distinct points on one line and* $\{p_6, \ldots, p_{10}\}$ *are distinct points on another line of* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$(q-1)(q^2+q+1)\frac{(q+1)q}{2}\binom{q}{5}^2(q^9+(q-1)q^4).$$

The number of weight 10 *codewords of* $C^{c\perp}_{2,4}$ *with support* $\{(w_1, p_1), \ldots, (w_{10}, p_{10})\}$ *such that* $\{p_1, \ldots, p_5\}$ *are distinct points on one line and* $\{p_6, \ldots, p_{10}\}$ *are distinct points on another line of* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$(q-1)(q^2+q+1)\frac{(q+1)q}{2}\binom{q}{5}^2 q^{10}.$$

PROOF. We first choose one of the q^2+q+1 rational points of $\mathbb{P}^2(\mathbb{F}_q)$. The number of pairs of $\mathbb{F}_q$-rational lines through this point is $\frac{(q+1)q}{2}$. The number of ways of choosing 5 points on each of these lines not including the intersection point is $\binom{q}{5}^2$.

By the previous lemma, if c is a weight 10 codeword of $C'^{\perp}_{2,4}$ with support given by $\{(w_1,p_1),\ldots,(w_{10},p_{10})\}$ satisfying the conditions of the proposition and nonzero coordinates $a_1,\ldots,a_{10}$, then

$$\sum_{i=1}^{10} a_i w_i^2 = 0.$$

The previous lemma shows that $\sum_{i=1}^{10} a_i x_i^2$ defines a plus quadric in $\mathbb{P}^9(\mathbb{F}_q)$. Such a quadric has $\frac{q^9-1}{q-1}+q^4$ $\mathbb{F}_q$-rational points. Taking scalar multiples of these projective points and adding in the possibility $(w_1,\ldots,w_{10})=(0,\ldots,0)$ gives $q^9+(q-1)q^4$ possibilities for $(w_1,\ldots,w_{10})$.

If c is a weight 10 codeword of $C^{c\perp}_{2,4}$ satisfying the conditions of this proposition then there are q^{10} possibilities for $(w_1,\ldots,w_{10})$.

Taking scalar multiples of these codewords gives an extra factor of $q-1$. □

Combining the counts for these different types of dual codewords is the final part of the proof of Theorems 63 and 64.

Before moving on to the next topic, we briefly mention two directions for future work. First, the main count given by Theorem 3 treats all anti-canonical models of del Pezzo surfaces of degree 2 the same. It would be interesting to separate the contribution coming from singular del Pezzo surfaces from the contribution of the smooth surfaces. Said another way, it would be interesting to determine how the trace of Frobenius acting on $\mathrm{Pic}(S)$ splits up as we vary over all homogeneous quartics in $\mathbb{P}(2,1,1,1)$ given by $w^2=f_4(x,y,z)$ where $f_4(x,y,z)$ is a smooth quartic on $\mathbb{P}^2(\mathbb{F}_q)$, not just a quartic with at most simple singularities. This would require some new extension of these ideas.

We have also seen that the Frobenius endomorphism induces a permutation of the (-1)-curves of S that is given by an element of the Weyl group of E_7. Theorem 3 gives a count closely related to the distribution of the values taken by the trace of this Weyl group element as we vary over all weak del Pezzo surfaces of degree 2 over $\mathbb{F}_q$. However, many conjugacy classes of the Weyl group of E_7 can have the same trace. It would be interesting to see if we could give exact counts for how often the permutation induced by Frobenius falls into each conjugacy class. We point out that the asymptotic version of this result mentioned at the end of Chapter 2 is given by an application of the Čebotarev density theorem, but it is unclear how to obtain exact counts in general.

CHAPTER 5

MacWilliams Identities for m-tuple Weight Enumerators

In this chapter we give a self-contained discussion of certain generalizations of the MacWilliams theorem. After this was written, Irfan Siap pointed out that the main generalization here, Theorem 102, is already present in the paper [**39**]. See this paper for another discussion of this result and some applications. For further applications of how this result can be used, and for other directions for possible generalization see Siap's thesis [**42**].

In a 1963 article [**33**], MacWilliams gave an identity relating the weight enumerator of a linear code to the weight enumerator of its dual code. Several authors have generalized this work in a few different directions. One type of generalization leads to weight enumerators in more than two variables, such as the Lee and complete weight enumerators, and to weight enumerators for codes defined over alphabets other than $\mathbb{F}_q$. Another type of generalization considered by several authors is to adapt the notion of weight to consider more than one codeword at a time. This leads to the generalized Hamming weights of Wei [**53**], and to the MacWilliams type results for m-tuple support enumerators of Kløve [**28**], Shiromoto [**41**], and Simonis [**44**]. Barg [**1**], and later Britz [**7**], generalized these results and gave matroid-theoretic proofs. Britz [**8**] also recently described new and broad connections between weight enumerators and Tutte polynomials of matroids.

We prove a MacWilliams type result that implies the two main theorems of Britz [**7**], which in turn imply the earlier results of Kløve [**28**], Shiromoto [**41**], and Barg [**1**]. While these earlier results mostly concern m-tuple generalizations of the MacWilliams

theorem for Hamming weight enumerators, we give the corresponding m-tuple generalization of the MacWilliams theorem for complete weight enumerators. Secondly, where the earlier results concern the analogue of the weight for m-tuples of codewords drawn from the same linear code C, our result applies for m-tuples of vectors, one each chosen from linear codes of length N, $C_1, \ldots, C_m$ that need not be the same.

In the last part of this chapter we mention some of the ways in which m-tuple support enumerators are used in the theory of linear codes and give some applications.

1. Statement of Results

We first give the necessary definitions to state MacWilliams' original theorem [**33**]. Let $\mathbb{F}_q$ be a finite field of q elements, N a nonnegative integer, and $C \subseteq \mathbb{F}_q^N$ a linear code. Let $|C|$ denote the number of codewords of C, and let $\langle a, b \rangle$ denote the usual pairing on $\mathbb{F}_q^N$. The *Hamming weight* of any $f \in \mathbb{F}_q^N$, denoted $\mathrm{wt}(f)$, is the number of nonzero coordinates of f. We define the *Hamming weight enumerator* of C,

$$\mathrm{W}_C(X, Y) = \sum_{c \in C} X^{N - \mathrm{wt}(c)} Y^{\mathrm{wt}(c)},$$

a homogeneous polynomial of degree N.

Theorem 100 (MacWilliams)**.** *Let $C \subseteq \mathbb{F}_q^N$ be a linear code and let $C^\perp$ be its dual code. Then*

$$\mathrm{W}_{C^\perp}(X, Y) = \frac{1}{|C|} \mathrm{W}_C(X + (q-1)Y, X - Y).$$

Many authors have considered not only the weights of individual codewords, but weights coming from m-tuples of codewords. We give some terminology from [**44**]. We will usually denote codewords with superscripts when we are considering more than one since we will use subscripts to denote the coordinates of a codeword.

Let $[N]$ denote $\{1, \ldots, N\}$. For $v = (v_1, \ldots, v_N) \in \mathbb{F}_q^N$, we define the *support* of v by $S(v) = \{e \in [N] \mid v_e \neq 0\}$. Note that $\mathrm{wt}(v) = |S(v)|$. If we consider a

codeword c as a $1 \times N$ row vector then $\mathrm{wt}(c)$ is the number of nonzero columns of this matrix. We define the *weight*, sometimes called the *effective length*, of an m-tuple of vectors $(v^1, \ldots, v^m) \in (\mathbb{F}_q^N)^m$ as the number of nonzero columns of the $m \times N$ matrix with rows $v^1, \ldots, v^m$. This is the size of the union of the supports of $v^1, \ldots, v^m$. For such an m-tuple $(v^1, \ldots, v^m)$ we define its *support*, $S(v^1, \ldots, v^m) = \bigcup_{i=1}^m S(v^i)$. For a subspace V of $\mathbb{F}_q^N$ we define its support as $S(V) = \bigcup_{v \in V} S(v)$. Note that $S(V)$ is the union of the supports of any set of vectors generating V. We define the *weight* of V as the size of this support.

We begin with the simplest generalization of the Hamming weight enumerator that considers multiple codewords at the same time. Let $C_1, \ldots, C_m$ be linear codes over $\mathbb{F}_q^N$. We define the m-tuple weight enumerator by

$$W^{[m]}_{C_1,\ldots,C_m}(X, Y) = \sum_{c^1 \in C_1} \cdots \sum_{c^m \in C_m} f(c^1, \ldots, c^m),$$

where if the m-tuple of vectors $(c^1, \ldots, c^m)$ has effective length equal to r, then $f(c^1, \ldots, c^m) = X^{N-r}Y^r$. One of our goals is to prove a version of the MacWilliams theorem for this m-tuple weight enumerator.

We now give one of the main theorems of [**7**]. For consistency we state this as an identity involving homogeneous polynomials, which is different from, but equivalent to, the original presentation. For $E \subseteq [N]$, let $A_E^{[m]}$ denote the number of ordered m-tuples of codewords in C whose support is E. We also define $2N$ variables $X_1, \ldots, X_N, Y_1, \ldots, Y_N$ that indicate whether a certain position is in the support of a given m-tuple of codewords. We define the *m-tuple support enumerator* of a linear code C of length N as

$$\begin{aligned} \mathrm{SE}_C^{[m]}(X_1, \ldots, X_N, Y_1, \ldots, Y_N) &= \sum_{E \subseteq [N]} A_E^{[m]} \prod_{i \in E} X_i \prod_{j \in [N] \setminus E} Y_j \\ &= \sum_{(c^1,\ldots,c^m) \in C^m} H(c^1, \ldots, c^m), \end{aligned}$$

where $H(c^1, \ldots, c^m) = \prod_{P=1}^{N} H_P(c^1, \ldots, c^m)$, and

$$H_P(c^1, \ldots, c^m) = \begin{cases} X_P \text{ if } (c_P^1, \ldots, c_P^m) = (0, \ldots, 0) \\ Y_P \text{ otherwise} \end{cases}.$$

Theorem 101 (Britz)**.** *Let $C \subseteq \mathbb{F}_q^N$ be a linear code and let $C^\perp$ be its dual code. Then*

$$\mathrm{SE}_{C^\perp}^{[m]}(X_1, \ldots, X_N, Y_1, \ldots Y_N) =$$
$$\frac{1}{|C|^m}\mathrm{SE}_C^{[m]}(X_1 + (q^m - 1)Y_1, \ldots, X_N + (q^m - 1)Y_N, X_1 - Y_1, \ldots, X_N - Y_N).$$

In this theorem the supports of m-tuples of codewords of C are related to the supports of m-tuples of codewords of $C^\perp$. This support enumerator keeps track of the supports, not just their sizes. However, given an m-tuple of codewords $c^1, \ldots, c^m$ written as an $m \times N$ matrix, this weight enumerator tells us only about the positions of the nonzero columns, not what these columns are.

We next define the complete weight enumerator of a linear code $C \subseteq \mathbb{F}_q^N$. Let $z_0 = 0, z_1, \ldots, z_{q-1}$ index the elements of $\mathbb{F}_q$. The complete weight enumerator of a code $C \subseteq \mathbb{F}_q^N$ is a homogeneous polynomial in q variables, $X_{z_0}, X_{z_1}, \ldots, X_{z_{q-1}}$, one for each of the q elements of $\mathbb{F}_q$. For $c = (c_1, \ldots, c_N) \in \mathbb{F}_q^N$, we define $F(c) = \prod_{i=0}^{q-1} X_{z_i}^{a_i(c)}$, where $a_i(c)$ is the number of $j \in [N]$ such that $c_j = z_i$. The *complete weight enumerator* of C is

$$\mathrm{CW}_C(X_{z_0}, \ldots, X_{z_{q-1}}) = \sum_{c \in C} F(c).$$

We also define the m-tuple complete weight enumerator of $C_1, \ldots, C_m$. Suppose $c^i \in C_i$ for $1 \leq i \leq m$. For any m-tuple $(c^1, \ldots, c^m)$, we consider the $m \times N$ matrix with rows $c^1, \ldots, c^m$. We define q^m variables,

$$X_{(z_0,z_0,\ldots,z_0)}, X_{(z_0,\ldots,z_0,z_1)}, \ldots, X_{(z_0,\ldots,z_0,z_n)}, X_{(z_0,z_0,\ldots,z_1,z_0)}, \ldots, X_{(z_{q-1},z_{q-1},\ldots,z_{q-1})},$$

one for each element of $\mathbb{F}_q^m$. When we have one variable for each possible m-tuple we always order the variables lexicographically.

Let $a_{(i_1,\ldots,i_m)}(c^1,\ldots,c^m)$ be the number of columns of this matrix that are equal to $(z_{i_1},\ldots,z_{i_m})^\intercal$. We are not concerned with the positions of the columns equal to a fixed m-tuple, only the number of such columns. Now let

$$F(c^1,\ldots,c^m) = \prod_{0\le i_1,\ldots,i_m<q} X_{(z_{i_1},\ldots,z_{i_m})}^{a_{(i_1,\ldots,i_m)}(c^1,\ldots,c^m)}.$$

We now define the *m-tuple complete weight enumerator* as

$$\mathrm{CW}_{C_1,\ldots,C_m}^{[m]}(X_{(z_0,\ldots,z_0)},\ldots,X_{(z_{q-1},\ldots,z_{q-1})}) = \sum_{c^1\in C_1}\cdots\sum_{c^m\in C_m} F(c^1,\ldots,c^m).$$

We also define a support analogue of the m-tuple complete weight enumerator of linear codes $C_1,\ldots,C_m$. The idea is to consider all possible m-tuples of codewords and to keep track of which of the q^m possible column vectors occurs in each of the N positions. This is a homogeneous polynomial in Nq^m variables $X_{P,(z_{i_1},\ldots,z_{i_m})}$ where $1\le P\le N$ and $(z_{i_1},\ldots,z_{i_m})\in\mathbb{F}_q^m$.

Suppose $c^i\in C_i$ for $1\le i\le m$ with $c^i=(c_1^i,\ldots,c_N^i)$. For any m-tuple $(c^1,\ldots,c^m)$, consider the $m\times N$ matrix with rows $c^1,\ldots,c^m$. Let

$$G(c^1,\ldots,c^m) = \prod_{P=1}^{N} G_P(c_P^1,\ldots,c_P^m),$$

where $G_P(c^1,\ldots,c^m) = G_P(c_P^1,\ldots,c_P^m) = X_{P,(c_P^1,\ldots,c_P^m)}$.

We now define the *m-tuple exact weight enumerator* of $C_1,\ldots,C_m$,

$$\begin{aligned}&\mathrm{EW}_{C_1,\ldots,C_m}^{[m]}(X_{1,(z_0,\ldots,z_0)},\ldots,X_{1,(z_{q-1},\ldots,z_{q-1})},\ldots,X_{N,(z_0,\ldots,z_0)},\ldots,X_{N,(z_{q-1},\ldots,z_{q-1})})\\ &= \sum_{c^1\in C_1}\cdots\sum_{c^m\in C_m} G(c^1,\ldots,c^m).\end{aligned}$$

For $m=1$ this weight enumerator coincides with the exact weight enumerator in the book of MacWilliams and Sloane [**34**]. We note that the m-tuple exact weight

enumerator contains strictly more information than the m-tuple complete weight enumerator since it keeps track not only of how many times each of the q^m possible columns occurs, but also in what positions they occur. It is clear that this weight enumerator completely specifies the words of each code $C_1, \ldots, C_m$.

We aim to prove the following generalizations of Theorem 1.

Theorem 102. *Let $C_1, \ldots, C_m$ be linear codes of length N, with dual codes $C_1^\perp, \ldots, C_m^\perp$, and let ψ be a non-trivial character on $\mathbb{F}_q$. Then*

$$\mathrm{EW}^{[m]}_{C_1^\perp,\ldots,C_m^\perp}(X_{1,(z_0,\ldots,z_0)}, \ldots, X_{1,(z_{q-1},\ldots,z_{q-1})}, \ldots, X_{N,(z_0,\ldots,z_0)}, \ldots, X_{N,(z_{q-1},\ldots,z_{q-1})}) =$$
$$\frac{1}{\prod_{i=1}^m |C_i|}\mathrm{EW}^{[m]}_{C_1,\ldots,C_m}(Y_{1,(z_0,\ldots,z_0)}, \ldots, Y_{1,(z_{q-1},\ldots,z_{q-1})}, \ldots, Y_{N,(z_0,\ldots,z_0)}, \ldots, Y_{N,(z_{q-1},\ldots,z_{q-1})}),$$

where if $(\alpha^1, \ldots, \alpha^m) \in (\mathbb{F}_q^N)^m$ and $\alpha_P = (\alpha_P^1, \ldots, \alpha_P^m)$ then,

$$Y_{P,(\alpha_P^1,\ldots,\alpha_P^m)} = \sum_{\beta=(\beta_1,\ldots,\beta_m)\in\mathbb{F}_q^m} \psi(\langle \alpha_P, \beta\rangle) X_{P,(\beta_1,\ldots,\beta_m)}.$$

The generalization for m-tuple complete weight enumerators follows easily from this.

Theorem 103. *Let $C_1, \ldots, C_m$ be linear codes of length N, with dual codes $C_1^\perp, \ldots, C_m^\perp$, and let ψ be a non-trivial character on $\mathbb{F}_q$. Then*

$$\mathrm{CW}^{[m]}_{C_1^\perp,\ldots,C_m^\perp}(X_{(z_0,\ldots,z_0)}, \ldots, X_{(z_{q-1},\ldots,z_{q-1})}) =$$
$$\frac{1}{\prod_{i=1}^m |C_i|}\mathrm{CW}^{[m]}_{C_1,\ldots,C_m}(Y_{(z_0,\ldots,z_0)}, \ldots, Y_{(z_{q-1},\ldots,z_{q-1})}),$$

where for $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m$,

$$Y_{(\alpha_1,\ldots,\alpha_m)} = \sum_{\beta=(\beta_1,\ldots,\beta_m)\in\mathbb{F}_q^m} \psi(\langle \alpha, \beta\rangle) X_{(\beta_1,\ldots,\beta_m)}.$$

We use this result to prove the following analogue for m-tuple weight enumerators.

Theorem 104. *Let $C_1, \ldots, C_m$ be linear codes over $\mathbb{F}_q^N$, with dual codes $C_1^\perp, \ldots, C_m^\perp$. Then*

$$\mathrm{W}^{[m]}_{C_1^\perp,\ldots,C_m^\perp}(X,Y) = \frac{1}{\prod_{i=1}^m |C_i|}\mathrm{W}^{[m]}_{C_1,\ldots,C_m}(X+(q^m-1)Y, X-Y).$$

This result allows one to compare the effective length of m-tuples of vectors drawn from different linear codes of the same length, and gives a generalization of an earlier result of Shiromoto [**41**] concerning the effective lengths of m-tuples of vectors from the same linear code C.

In the final part of the paper we discuss extensions to r-th support weight enumerators. Wei [**53**] first considered the r-th generalized Hamming Weight $d_r(C)$, which is the smallest effective length of an r-tuple of codewords of C that generate an r-dimensional subcode of C. Kløve [**28**] was the first to prove MacWilliams type relations for these effective length distributions. We first define the r-th support weight distribution $\{A_i^{(r)} \mid \ i \geq 0\}$ of C where $A_i^{(r)}$ is the number of r-dimensional subspaces of C that have support of size exactly i.

We define the *r-th support weight enumerator* of a linear code C,

$$\mathrm{W}_C^{(r)}(X,Y) = \sum_{i=0}^{N} A_i^{(r)} X^{N-i} Y^i.$$

Britz [**7**] gave a generalization of this weight enumerator that considers not only the dimension of the subcode but also which of the coordinates in $[N]$ lie in the support of the subcode. We consider an analogue of this r-th support weight enumerator for linear codes of length N, $C_1, \ldots, C_m$, not necessarily equal, and see that things do not carry over so neatly in this setting. We discuss this issue and give some applications of our results.

We can express an m-tuple of elements of $\mathbb{F}_q^N$ as the rows of an $m \times N$ matrix. A column of this matrix gives an m-tuple $(\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m$. If we choose a basis for $\mathbb{F}_q^m$, we can think of this m-tuple as an element of $\mathbb{F}_q^m$. The resulting code over $\mathbb{F}_q^m$ is no longer linear since it is not closed under scalar multiplication by elements

of $\mathbb{F}_q^m \setminus \mathbb{F}_q$, but it is $\mathbb{F}_q$-linear. Codes of this type are often called *additive* codes. We can then think of Theorem 104 as a kind of MacWilliams theorem for additive codes over $\mathbb{F}_q^m$. We will not pursue this interpretation further here, but it may be useful in future work.

2. The Proof of Theorem 102

We prove Theorem 102 on m-tuple exact weight enumerators using an argument similar in spirit to one of the original proofs of the MacWilliams identity [**33**]. Similar ideas have been used by Britz and others [**7, 20**]. We apply discrete Poisson summation and a simple lemma on characters.

Lemma 105 (Discrete Poisson summation)**.** *Let G be a finite abelian group, $H \subset G$ a subgroup, $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ the character group of G, and $H^* = \{\hat{g} \in \widehat{G} \mid \forall h \in H,\ \widehat{g}(h) = 1\}$ the annihilator of H in $\widehat{G}$. For any function ϕ on G define the Fourier transform of ϕ to be the function on $\widehat{G}$*

$$\hat{\phi}(\hat{g}) = \sum_{g \in G} \hat{g}(g)\phi(g).$$

Then

$$[G : H] \sum_{h \in H} \phi(h) = \sum_{h^* \in H^*} \hat{\phi}(h^*).$$

See Chapter 12 of [**48**] for a proof.

In this m-tuple weight enumerator setting we let $G = (\mathbb{F}_q^N)^m$ and let ψ be a non-trivial character on $\mathbb{F}_q$. We identify $\widehat{G}$ and G by identifying the element $g = (g^1, \ldots, g^m) \in (\mathbb{F}_q^N)^m$ with the character that takes $h = (h^1, \ldots, h^m) \in (\mathbb{F}_q^N)^m$ to $\psi(\langle h, g \rangle)$. Let $C_1, \ldots, C_m$ be linear codes of length N. Consider the subgroup of G^m that consists of elements of the form $(c^1, \ldots, c^m)$ where $c^i \in C_i$. This subgroup has index $q^{Nm} \left(\prod_{i=1}^m |C_i|\right)^{-1} = \prod_{i=1}^m |C_i^\perp|$.

Proof of Theorem 102. Let

$$\phi(c^1,\ldots,c^m) = G(c^1,\ldots,c^m) = \prod_{P=1}^{N} G_P(c^1,\ldots,c^m),$$

where the function G_P is defined in the previous section. Now we see that

$$\hat{\phi}(\hat{g}) = \sum_{g\in(\mathbb{F}_q^N)^m} \psi(\langle g,\hat{g}\rangle)\phi(g).$$

Summing over all $(c^1,\ldots,c^m)$ with $c^i \in C_i$ gives

$$\sum_{c^1\in C_1,\ldots,c^m\in C_m} \phi(c^1,\ldots,c^m) = \mathrm{EW}^{[m]}_{C_1,\ldots,C_m}(X_{1,(z_0,\ldots,z_0)},\ldots,X_{N,(z_{q-1},\ldots,z_{q-1})}).$$

Discrete Poisson summation implies that this is equal to

$$\frac{1}{\prod_{i=1}^m |C_i^\perp|} \sum_{d^1\in C_1^\perp,\ldots,d^m\in C_m^\perp} \hat{\phi}(d^1,\ldots,d^m).$$

We now consider the coordinates of $\hat{\phi}(d^1,\ldots,d^m)$ one at a time. Note that

$$\begin{aligned}\hat{\phi}(d^1,\ldots,d^m) &= \sum_{(g^1,\ldots,g^m)\in(\mathbb{F}_q^N)^m} \prod_{i=1}^m \psi(\langle d^i,g^i\rangle)\phi(g^1,\ldots,g^m)\\ &= \sum_{(g^1,\ldots,g^m)\in(\mathbb{F}_q^N)^m} \prod_{i=1}^m \psi(\langle d^i,g^i\rangle)\prod_{P=1}^N G_P(g_P^1,\ldots,g_P^m),\end{aligned}$$

where $g^i = (g_1^i,\ldots,g_n^i)$.

We can switch the order of the sum and product and still account for every $(g^1,\ldots,g^m)\in(\mathbb{F}_q^N)^m$ exactly once. This sum is equal to

$$\prod_{P=1}^N \sum_{(g_P^1,\ldots,g_P^m)\in\mathbb{F}_q^m} \prod_{i=1}^m \psi(d_P^i,g_P^i)G_P(g_P^1,\ldots,g_P^m).$$

Let $g_P = (g_P^1, \ldots, g_P^m)$ and $d_P = (d_P^1, \ldots, d_P^m)$. We can rewrite the previous sum as

$$\prod_{P=1}^{N} \sum_{g_P \in \mathbb{F}_q^m} \psi(\langle d_P, g_P \rangle) X_{P,(g_P^1,\ldots,g_P^m)},$$

completing the proof. □

3. Applications of Theorem 102 to Other Weight Enumerators

In this section we deduce Theorem 103 and then Theorem 101 from Theorem 102, and then deduce Theorem 104 from Theorem 103.

Proof of Theorem 103. For all P satisfying $1 \le P \le N$ and all $(i_1, \ldots, i_m)$ with $0 \le i_1, \ldots, i_m < q$, set $X_{P,(z_{i_1},\ldots,z_{i_m})} = X_{(z_{i_1},\ldots,z_{i_m})}$. By definition, for any fixed $(i_1, \ldots, i_m)$ the $Y_{P,(z_{i_1},\ldots,z_{i_m})}$ for $1 \le P \le N$ are all equal. We also see that for all P satisfying $1 \le P \le N$ we have $G_P(c^1, \ldots, c^m) = X_{(c_P^1,\ldots,c_P^m)}$. Therefore

$$G(c^1, \ldots, c^m) = \prod_{0 \le i_1,\ldots,i_m < q} X_{(z_{i_1},\ldots,z_{i_m})}^{a_{(i_1,\ldots,i_m)}(c^1,\ldots,c^m)}.$$

Taking the sum over all m-tuples satisfying $c^1 \in C_1, \ldots, c^m \in C_m$ gives the weight enumerator $\mathrm{CW}_{C_1,\ldots,C_m}^{[m]}(X_{(z_0,\ldots,z_0)}, \ldots, X_{(z_{q-1},\ldots,z_{q-1})})$, so the left-hand sides of the identities in the two theorems are equal. The observation that $Y_{P,(z_{i_1},\ldots,z_{i_m})} = Y_{(z_{i_1},\ldots,z_{i_m})}$ for all P completes the proof. □

We recall a useful lemma on sums of characters.

Lemma 106. *Suppose $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m \setminus (0, \ldots, 0)$. Let ψ be a non-trivial character on $\mathbb{F}_q$. Then*

$$\sum_{\beta=(\beta_1,\ldots,\beta_m) \in \mathbb{F}_q^m \setminus (0,\ldots,0)} \psi(\langle \alpha, \beta \rangle) = -1.$$

PROOF. The map $\beta \to \psi(\langle \alpha, \beta \rangle)$ is a character on the finite additive group $\mathbb{F}_q^m$. Therefore, the sum of this character over all β vanishes unless it is the trivial character, which is the case if and only if $\alpha = (0, \ldots, 0)$. We see that

$$\sum_{\beta=(\beta_1,\ldots,\beta_m)\in\mathbb{F}_q^m\setminus(0,\ldots,0)} \prod_{i=1}^{m} \psi(\alpha_i\beta_i) = 0 - \prod_{i=1}^{m} \psi(0) = -1.$$

□

PROOF OF THEOREM 101. Suppose for each i satisfying $1 \leq i \leq m$, $C_i = C_1$. For convenience we write $C := C_1$. For each $P \in [1, N]$ set $X_{P,(0,\ldots,0)} = X_P$ and for all other m-tuples, set $X_{P,(i_1,\ldots,i_m)} = Y_P$.

First consider

$$Y_{P,(z_0,\ldots,z_0)} = \sum_{\beta=(\beta_1,\ldots,\beta_m)\in\mathbb{F}_q^m} X_{P,(\beta_1,\ldots,\beta_m)}.$$

This is equal to $X_P + (q^m - 1)Y_P$.

Suppose $\alpha_P = (\alpha_P^1, \ldots, \alpha_P^m) \neq (0, \ldots, 0)$ and consider

$$Y_{P,(\alpha_P^1,\ldots,\alpha_P^m)} = \sum_{\beta=(\beta_1,\ldots,\beta_m)\in\mathbb{F}_q^m} \psi(\langle \alpha_P, \beta \rangle) X_{P,(\beta_1,\ldots,\beta_m)}.$$

In this case, the map that takes $\beta \in \mathbb{F}_q^m$ to $\psi(\langle \beta, \alpha_P \rangle)$ is a non-trivial character on $\mathbb{F}_q$. From the $\beta = (0, \ldots, 0)$ term we get X_P and from the other terms we get

$$Y_P \sum_{\beta\neq(0,\ldots,0)} \psi(\langle \alpha_P, \beta \rangle) = -Y_P,$$

by the above lemma. Therefore, $Y_{P,(\alpha_P^1,\ldots,\alpha_P^m)} = X_P - Y_P$.

Collecting terms completes the proof. □

PROOF OF THEOREM 104. For any m-tuple $(i_1, \ldots, i_m) \neq (0, \ldots, 0)$ satisfying $0 \leq i_1, \ldots, i_m < q$, set $X_{(z_{i_1},\ldots,z_{i_m})}$ equal to Y. Set $X_{(z_0,\ldots,z_0)} = X$. We note that

$$Y_{(z_0,\ldots,z_0)} = \sum_{(z_{i_1},\ldots,z_{i_m})\in\mathbb{F}_q^m} X_{(z_{i_1},\ldots,z_{i_m})} = X + (q^m - 1)Y.$$

Consider an m-tuple $(\alpha_1, \ldots, \alpha_m) \neq (0, \ldots, 0)$ satisfying $0 \leq \alpha_1, \ldots, \alpha_m < q$. By the lemma, we have

$$Y_{(\alpha_1,\ldots,\alpha_m)} = X + \sum_{\beta=(\beta_1,\ldots,\beta_m)\neq(0,\ldots,0)} \psi(\langle \alpha, \beta \rangle) Y = X - Y.$$

We note that $a_{(0,\ldots,0)}(c^1, \ldots, c^m)$ just counts the number of columns of the $m \times N$ matrix with rows $c^1, \ldots, c^m$ that are equal to $(0, \ldots, 0)^\intercal$. Collecting terms completes the proof.

□

4. Support Weight Enumerators and Applications

Several authors have studied weight enumerators from m-tuples of codewords from a single linear code C where these m-tuples are grouped by the dimension of the subcode that they generate. This leads to the definition of generalized Hamming weights, which have been studied extensively [**26, 53**].

Definition. *Let C be a linear code of dimension k. For each r satisfying $1 \leq r \leq k$ we define the* r-th generalized Hamming weight of C, *denoted $d_r(C)$, to be the minimum size of the support of an r-tuple of codewords of C that generate an r-dimensional subcode of C.*

We can now give a definition of r-th generalized Hamming weights for an r-tuple of not necessarily equal codes $C_1, \ldots, C_r$.

Definition. *Let $C_1, \ldots, C_r$ be not necessarily equal linear codes of the same length N. Suppose there exists an r-tuple of codewords $c^1, \ldots, c^r$ where $c^i \in C_i$ that span an r-dimensional subspace of $\mathbb{F}_q^N$. Then we define the* r-th generalized Hamming weight for $C_1, \ldots, C_r$ *to be the minimum size of the support of such an r-dimensional subspace.*

We note that $d_r(C_1, \ldots, C_r)$ does not depend on the order of the codes, only on the underlying multiset of codes. We also note that codewords $c^1, \ldots, c^r$ where $c^i \in C_i$ can generate an r-dimensional subspace of $\mathbb{F}_q^N$ that is not a subspace of any particular C_i. In the case where for each $i \in [1, m]$, $C_i = C_1$ and C_1 has dimension k, we see that for $r \leq k$ this is exactly $d_r(C_1)$.

First, we recall the following result of Wei [**53**].

Proposition 107 (Wei)**.** *Suppose that C is a code over $\mathbb{F}_q$ of length N and dimension k. Then for each r satisfying $1 \leq r \leq k-1$, $d_r(C) < d_{r+1}(C)$.*

A simple example shows that the analogue of this result does not hold when the codes $C_1, \ldots, C_r$ are not equal. For example, let C_1 be the binary repetition code of length N and C_2 be $\mathbb{F}_2^N$. We see that $d_2(C_1, C_2) = N$, since any two-dimensional subspace of $\mathbb{F}_2^N$ spanned by $c^1 \in C_1$ and $c^2 \in C_2$ must have c^1 nonzero and therefore equal to $(1, \ldots, 1)$. So, this subspace has weight N. We also note that $d_r(C_1, C_2, \ldots, C_2) = N$ for any $r \in [2, N]$ where C_2 is repeated $r-1$ times, since the nonzero vector $c^1 \in C_1$ must be $(1, \ldots, 1)$.

There is an analogue of the m-tuple weight enumerator that keeps track of the effective length of collections of codewords of C that generate an r-dimensional subcode. The main fact that allows one to adapt the MacWilliams theorem for m-tuple support enumerators to give information about only m-tuples of codewords of C that span a subspace of dimension r is the following classical result.

Proposition 108. *Let D be an r-dimensional subspace of $\mathbb{F}_q^N$. The number of ordered m-tuples of vectors $(d^1, \ldots, d^m) \in D^m$ that span D is independent of D. It is equal to $[m]_r := \prod_{i=0}^{r-1}(q^m - q^i)$.*

Let C be a linear code of length N and dimension k over $\mathbb{F}_q$. It is now an elementary observation that

$$W_C^{[m]}(X,Y) = \sum_{r=0}^{k} [m]_r W_C^{(r)}(X,Y).$$

Applying the MacWilliams theorem to this weight enumerator gives the following result originally due to Kløve [**28**].

Proposition 109 (Kløve)**.** *Let C be a linear code of length N and dimension k over $\mathbb{F}_q$. Then for any $m \geq 1$,*

$$\sum_{r=0}^{N-k} [m]_r W_{C^\perp}^{(r)}(X,Y) = \frac{1}{q^{km}} \sum_{r=0}^{k} [m]_r W_C^{(r)}(X + (q^m - 1)Y, X - Y).$$

Adapting this result for m-tuples of words from different codes is not so straightforward. Suppose we have linear codes $C_1, \ldots, C_m$ that are not necessarily the same and want to consider only m-tuples of codewords $(c^1, \ldots, c^m)$ with $c^i \in C_i$ that span a particular r-dimensional subspace D of $\mathbb{F}_q^N$. It is no longer the case that the number of m-tuples spanning D depends only on r. For example, if we choose a one-dimensional space D, the number of m-tuples spanning D depends on the number of C_i that contain D. In general, for a particular space, in order to know the number of m-tuples of codewords that span it, we must know the dimension of the intersection of this space with each of the codes C_i.

We next consider one of the simplest examples with unequal codes. We will see that the analogue of Proposition 109 is much more complicated. Let C_1 and C_2 be distinct linear codes over $\mathbb{F}_q$ of the same length N. Suppose that C_1 has dimension k, C_2 has dimension l, and $C_1 \cap C_2$ has dimension s. For each subspace of the code generated by C_1 and C_2 that is spanned by some pair (c^1, c^2) with $c^1 \in C_1$ and $c^2 \in C_2$, we can ask for the number of such pairs of codewords that span this

subspace. We see that only the pair $((0,\ldots,0),(0,\ldots,0))$ spans the zero-dimensional subspace consisting only of the zero codeword.

We first consider one-dimensional spaces. Suppose we have a one-dimensional subspace of $C_1 \cap C_2$. By Proposition 108, this is generated by $[2]_1 = q^2 - 1$ pairs. A one-dimensional subspace of C_1 that does not lie in $C_1 \cap C_2$ must have a zero-dimensional intersection with it, so can only be generated by a pair of the form $(c^1, 0)$ where c^1 lies in the subspace. There are $q-1$ nonzero vectors in a one-dimensional subspace of $\mathbb{F}_q^N$. A similar statement holds for one-dimensional subspaces of C_2 that do not lie in $C_1 \cap C_2$. Adding these up gives

$$(q-1)W_{C_1}^{(1)}(X,Y) + (q-1)W_{C_2}^{(1)} + (q-1)^2 W_{C_1\cap C_2}^{(1)}(X,Y),$$

since we have taken $2(q-1)$ of the pairs of vectors generating subspaces in $C_1 \cap C_2$ and $q^2 - 1 - 2(q-1) = (q-1)^2$.

We next consider two-dimensional subspaces of the code generated by C_1 and C_2. We note that $C_1 \setminus \{C_1 \cap C_2\} = C_1 \setminus C_2$.

Proposition 110. *Let C_1 and C_2 be linear codes over $\mathbb{F}_q$ of length N and dimensions k and l, respectively. Suppose that $C_1 \cap C_2$ has dimension s. Then*

$$\begin{aligned} W_{C_1,C_2}^{[2]}(X,Y) &= X^N + (q-1)\left(W_{C_1}^{(1)}(X,Y) + W_{C_2}^{(1)}(X,Y)\right) + (q-1)^2 W_{C_1\cap C_2}^{(1)}(X,Y) \\ &+ (q^2-1)(q^2-q)W_{C_1\cap C_2}^{(2)}(X,Y) \\ &+ q(q-1)^2\left(W_{C_1\setminus C_2}^{(2)}(X,Y) + W_{C_2\setminus C_1}^{(2)}(X,Y)\right) \\ &+ (q-1)^2 W_{\langle C_1,C_2\rangle\setminus\{C_1\cup C_2\}}^{(2)}(X,Y), \end{aligned}$$

where

$$W_{C_i\setminus C_1\cap C_2}^{(2)}(X,Y) = \sum_{i=0}^{N} A_i^{(2)} X^{N-i} Y^i,$$

and $A_i^{(2)}$ *denotes the number of two-dimensional subcodes of* C_i *that have a one-dimensional intersection with* $C_1 \cap C_2$ *and weight* i*, and*

$$W^{(2)}_{\langle C_1,C_2\rangle\setminus\{C_1\cup C_2\}}(X,Y) = \sum_{i=0}^{N} B_i^{(2)} X^{N-i}Y^i,$$

where $B_i^{(2)}$ *denotes the number of two-dimensional subcodes of the code spanned by* C_1 *and* C_2 *but are not subcodes of either* C_1 *or* C_2*, that have weight* i*.*

PROOF. The number of pairs of vectors generating a two-dimensional subspace of $C_1 \cap C_2$ is $[2]_2 = (q^2-1)(q^2-q)$. The number of such subspaces is given by $((q^s-1)(q^s-q))/((q^2-1)(q^2-q))$. We next consider two-dimensional subspaces of C_1 that are not contained in $C_1 \cap C_2$. If such a space can be generated by a pair (c^1, c^2) then $c^2 \in C_1 \cap C_2$. Given such a space, if we first choose c^2 there are $q^2 - q$ choices for c^1, since the space contains q^2 total vectors. There are $(q^s-1)/(q-1)$ one-dimensional subspaces of $C_1 \cap C_2$ and $((q^s-1)(q^s-q))/((q^2-1)(q^2-q))$ two-dimensional subspaces. There are $((q^k-1)(q^k-q))/((q^2-1)(q^2-q))$ two-dimensional subspaces of C_1 each containing $(q^2-1)/(q-1) = q+1$ one-dimensional subspaces. Therefore, there are

$$\frac{(q^k-1)(q^k-q)}{(q^2-1)(q^2-q)} \cdot \frac{(q+1)(q-1)}{q^k-1} = \frac{q^{k-1}-1}{q-1}$$

two-dimensional subspaces of C_1 containing a given one-dimensional subspace of $C_1 \cap C_2$. We see that $(q^{s-1}-1)/(q-1)$ of these are actually two-dimensional subspaces of $C_1 \cap C_2$. Therefore, we have

$$\frac{q^{k-1}-1-(q^{s-1}-1)}{q-1} \cdot \frac{q^s-1}{q-1} = \frac{(q^k-q^s)(q^s-1)}{q(q-1)^2}$$

two-dimensional subspaces of $C_1 \setminus C_2$ that can be generated by a pair (c^1, c^2) with $c^1 \in C_1,\ c^2 \in C_2$. For each such space there are $(q^2-q)(q-1)$ pairs generating it, giving a total of $(q^k-q)(q^s-1)$ pairs generating such subspaces. This is the same

as the total number of pairs $c^1 \in C_1 \setminus C_2,\ c^2 \in C_1 \cap C_2$, giving a useful verification of this count. We similarly count $(q^l - q^s)(q^s - 1)$ pairs of vectors that generate a two-dimensional subspace of $C_2 \setminus C_1$.

Using similar techniques we see that there are $(q^k - q^s)(q^l - q^s)/(q-1)^2$ subspaces of the code generated by C_1 and C_2 that have trivial intersection with $C_1 \cap C_2$, and that each of these is generated by $(q-1)^2$ pairs (c^1, c^2) with $c^i \in C_i$. We omit the details. □

We can now apply Theorem 104 to this expression and see that this is equal to $\left(|C_1^\perp||C_2^\perp|\right)^{-1}$ times the right hand side where each C_i is replaced with $C_i^\perp,\ C_1 \cap C_2$ is replaced with $C_1^\perp \cap C_2^\perp$ and (X, Y) is replaced with $(X + (q^2-1)Y, X - Y)$.

We give an example in order to make this more concrete. We give binary codes of length 6, C_1 and C_2 in terms of generator matrices,

$$C_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We see that $C_1 \cap C_2$ is the one-dimensional subspace generated by $(1,1,1,1,1,1)$, and that

$$C_1^\perp = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad C_2^\perp = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

showing that C_1 is not self-dual, but is permutation equivalent to its dual.

We compute

$$\begin{aligned} W^{(1)}_{C_1}(X,Y) &= 3X^4Y^2 + 3X^2Y^4 + Y^6,\ W^{(1)}_{C_2}(X,Y) = 2X^3Y^3 + Y^6, \\ W^{(1)}_{C_1\cap C_2}(X,Y) &= Y^6,\ W^{(2)}_{C_1\cap C_2}(X,Y) = 0,\ W^{(2)}_{C_1\setminus C_2}(X,Y) = 3Y^6, \\ W^{(2)}_{C_2\setminus C_1}(X,Y) &= Y^6,\ W^{(2)}_{\langle C_1,C_2\rangle\setminus\{C_1\cup C_2\}}(X,Y) = 3(X^3Y^3 + X^2Y^4 + XY^5 + Y^6). \end{aligned}$$

The above proposition now gives

$$W^{[2]}_{C_1,C_2}(X,Y) = X^6 + 3X^4Y^2 + 5X^3Y^3 + 6X^2Y^4 + 3XY^5 + 14Y^6.$$

Applying Theorem 104 gives

$$W^{[2]}_{C_1^\perp,C_2^\perp}(X,Y) = X^6 + 12X^4Y^2 + 6X^3Y^3 + 39X^2Y^4 + 42XY^5 + 28Y^6.$$

We can also see this by noting that $C_1^\perp \cap C_2^\perp = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$, and performing an analysis similar to the one above. We can compute each of the polynomials in the statement of the theorem, add them up with the proper constants and get $W^{[2]}_{C_1^\perp,C_2^\perp}(X,Y)$.

We state a corollary of Theorem 104 separately.

Corollary 111. *Let $m \geq 1$ and C be a linear code of length N over $\mathbb{F}_q$. Then*

$$W^{[2m]}_{C,\ldots,C,C^\perp,\ldots,C^\perp}(X,Y) = \frac{1}{q^{Nm}} W^{[2m]}_{C,\ldots,C,C^\perp,\ldots,C^\perp}(X + (q^m-1)Y, X - Y),$$

where C and $C^\perp$ are each repeated m times.

A self-dual code C must have its m-tuple weight enumerators invariant under certain transformations. This is the main idea behind Gleason's theorem giving necessary conditions for the weight enumerators of self-dual codes [**26, 38**]. This corollary lets us produce polynomials that are invariant under the m-tuple analogue of the MacWilliams transformation, but are not necessarily the m-tuple weight enumerators

of self-dual codes, in fact, are not necessarily the m-tuple weight enumerators of any single code C.

Let C_3 be the binary code with generator matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$. Then,

$$\begin{aligned} W^{[2]}_{C_3,C_3^\perp}(X,Y) &= X^6 + 5X^4Y^2 + 8X^3Y^3 + 11X^2Y^4 + 24XY^5 + 15Y^6 \\ &= \frac{1}{2^6} W^{[2]}_{C_3,C_3^\perp}(X+3Y, X-Y), \end{aligned}$$

but this cannot be the 2-tuple weight enumerator of any code. This is because for a binary code C,

$$W^{[2]}_C(X,Y) = \sum_{r=0}^{2} [2]_r W^{(r)}_C(X,Y),$$

so for each $i \in [1,N]$ the X^iY^{N-i} coefficient must be divisible by 3, but the X^4Y^2 term has coefficient 5.

Let C_4 have generator matrix $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$. This code has

$$W^{[2]}_{C_4,C_4^\perp}(X,Y) = X^6 + 9X^4Y^2 + 27X^4Y^2 + 9Y^6,$$

which is the 2-tuple weight enumerator of the self dual code C_5 with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We can also ask, given a polynomial that arises as $W^{[m]}_C(X,Y)$ for some C, whether we can characterize the m-tuples of codes $C_1, \ldots, C_m$ that give the same m-tuple weight enumerator.

We can ask questions of the following type. Given m and q, which homogeneous polynomials $W(X,Y)$ of degree N are invariant under the transformation sending it

to $q^{\frac{-Nm}{2}} W(X+(q^m-1)Y, X-Y)$? This is asking for a kind of analogue of Gleason's theorem for these m-tuple weight enumerators. For more information on this subject see the work of Nebe, Rains and Sloane [**38**]. We know that there are polynomials invariant under this transformation that cannot be the m-tuple weight enumerator of any code, for example polynomials with multiple coefficients not divisible by q^2-1. What further necessary conditions can we find for such an invariant polynomial to occur as the m-tuple weight enumerator of a code? We would like to be able to use results of this type to aid in the classification of self-dual codes, and in more general classification problems.

We note that C_5 has the same weight enumerator as C_1, but that these two codes have different 2-tuple weight enumerators. This implies that the m-tuple weight enumerator of C does not determine the $(m+1)$-tuple weight enumerator. It is less clear whether it is possible for two codes to have the same $(m+1)$-tuple weight enumerators and different m-tuple weight enumerators. Extensive computer search produced the following example (and many others). Let D_1 be the binary code of length 12 and dimension 6 with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix},$$

and let D_2 be the binary code of length 12 and dimension 6 with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

We compute that D_1 has Hamming weight enumerator

$$X^{12}+X^{10}Y^2+3X^9Y^3+6X^8Y^4+15X^7Y^5+14X^6Y^6+9X^5Y^7+9X^4Y^8+5X^3Y^9+X^2Y^{10},$$

and that

$$W_{D_1}^{[2]}(X,Y) = X^{12} + 3X^{10}Y^2 + 9X^9Y^3 + 24X^8Y^4 + 75X^7Y^5 + 162X^6Y^6$$
$$+399X^5Y^7 + 771X^4Y^8 + 957X^3Y^9 + 975X^2Y^{10} + 576XY^{11} + 144Y^{12}.$$

We compute that D_2 has Hamming weight enumerator

$$X^{12}+X^{10}Y^2+3X^9Y^3+8X^8Y^4+11X^7Y^5+12X^6Y^6+17X^5Y^7+7X^4Y^8+X^3Y^9+3X^2Y^{10},$$

and the same 2-tuple weight enumerator as D_1. Therefore, $(m+1)$-tuple weight enumerators do not determine m-tuple weight enumerators. This is related to recent work of Britz [**8**], in which he shows that for a k-dimensional linear code C the collection of m-tuple weight enumerators for all m satisfying $1 \leq m \leq k$ is equivalent to the Tutte polynomial of the matroid associated to C.

5. The Repetition Code and the Parity Check Code

We end this chapter with one more type of example. Let R be the q-ary repetition code of length N, that is, the one-dimensional code generated by $(1, 1, \ldots, 1)$. Then

$R^\perp$ is the parity check code, which consists of all vectors of $\mathbb{F}_q^N$, $(c_1, \ldots, c_N)$ with $c_1 + \cdots + c_N = 0$ in $\mathbb{F}_q$. Let $C_1, \ldots, C_m$ be linear codes of length N over $\mathbb{F}_q$. It is easy to see how to determine higher weight enumerators involving R, and less obvious how to determine weight enumerators involving $R^\perp$. Theorem 104 gives one way to solve this problem.

For any $m \geq 1$,

$$W^{[m+1]}_{C_1,\ldots,C_m,R}(X,Y) = W^{[m]}_{C_1,\ldots,C_m}(X,Y) + (q-1)\prod_{i=1}^{m} |C_i| Y^N,$$

since we can either choose the all zero codeword from R, giving the first term, or one of the $q-1$ words of weight N, giving the second term. Similarly, we see that for any $m \geq 1$,

$$W^{[m+s]}_{C_1,\ldots,C_m,R,\ldots,R}(X,Y) = W^{[m]}_{C_1,\ldots,C_m}(X,Y) + (q^s-1)\prod_{i=1}^{m} |C_i| Y^N,$$

where R is repeated s times. More generally, the same result holds if R is any one-dimensional code over $\mathbb{F}_q$ generated by a vector with all nonzero coordinates. This will be our assumption on R from now on.

Proposition 112. *Let $C_1, \ldots, C_m$ be linear codes of length N over $\mathbb{F}_q$ and let R be a one-dimensional code over $\mathbb{F}_q$ of length N generated by $(c_1, \ldots, c_N)$, where each c_i is nonzero. Then*

$$\begin{aligned} W^{[m+s+t]}_{C_1,\ldots,C_m,R,\ldots,R,R^\perp,\ldots,R^\perp}(X,Y) &= (q^s-1)q^{(N-1)t}\prod_{i=1}^{m}|C_i|Y^N + \frac{(q^t-1)}{q^t}(X-Y)^N \\ &+ \frac{1}{q^t} W^{[m]}_{C_1,\ldots,C_m}(X+(q^t-1)Y, q^t Y), \end{aligned}$$

where R is repeated s times and $R^\perp$ is repeated t times.

PROOF. We consider $W^{[m+s+t]}_{C_1,\ldots,C_m,R,\ldots,R,R^\perp,\ldots,R^\perp}(X,Y)$, where R is repeated s times and $R^\perp$ is repeated t times. From the previous paragraph we have

$$W^{[m+s+t]}_{C_1,\ldots,C_m,R,\ldots,R,R^\perp,\ldots,R^\perp}(X,Y) = W^{[m+t]}_{C_1,\ldots,C_m,R^\perp,\ldots,R^\perp}(X,Y) + (q^s-1)q^{(N-1)t}\prod_{i=1}^m |C_i|Y^N,$$

since $|R^\perp| = q^{(N-1)}$. We apply Theorem 104 and see that

$$\begin{aligned} W^{[m+t]}_{C_1,\ldots,C_m,R^\perp,\ldots,R^\perp}(X,Y) &= \frac{1}{q^t\prod_{i=1}^m |C_i^\perp|} W^{[m+t]}_{C_1^\perp,\ldots,C_m^\perp,R,\ldots,R}(X+(q^{m+t}-1)Y, X-Y) \\ = \quad & \frac{1}{q^t\prod_{i=1}^m |C_i^\perp|}\big(W^{[m]}_{C_1^\perp,\ldots,C_m^\perp}(X+(q^{m+t}-1)Y, X-Y) + (q^t-1)\prod_{i=1}^m |C_i|^\perp (X-Y)^N\big). \end{aligned}$$

Applying Theorem 104 one more time gives

$$\begin{aligned} & \frac{W^{[m]}_{C_1^\perp,\ldots,C_m^\perp}(X+(q^{m+t}-1)Y, X-Y)}{q^t\prod_{i=1}^m |C_i^\perp|} \\ = \quad & \frac{W^{[m]}_{C_1,\ldots,C_m}(X+(q^{m+t}-1)Y+(q^m-1)(X-Y), X+(q^{m+t}-1)Y-(X-Y))}{q^t\prod_{i=1}^m |C_i||C_i|^\perp} \\ = \quad & \frac{1}{q^t q^{Nm}} W^{[m]}_{C_1,\ldots,C_m}(q^m(X+(q^t-1)Y), q^m(q^tY)) \\ = \quad & \frac{1}{q^t} W^{[m]}_{C_1,\ldots,C_m}(X+(q^t-1)Y, q^tY). \end{aligned}$$

□

In certain cases it is not difficult to work out this proposition directly without use of the MacWilliams theorem and its generalizations. For example this is not difficult when $m=1,\ q=2,\ s=0$, and $t=1$. In this case $R^\perp$ is the even weight subcode of $\mathbb{F}_2^N$ and we get

$$W^{[2]}_{C_1,R^\perp}(X,Y) = \frac{(X-Y)^N}{2} + \frac{W_{C_1}(X+Y,2Y)}{2} = W_{R^\perp}(X,Y) + \frac{W^{(1)}_{C_1}(X+Y,2Y)}{2},$$

since $W_{R^\perp}(X,Y) = \frac{(X-Y)^N+(X+Y)^N}{2}$.

Proposition 112 gives a unified way to compute some of these more complicated higher weight enumerators. Hopefully results of this type can be used to give further conditions on the existence of codes with certain weight enumerators or parameters.

CHAPTER 6

Rational Points on Complete Intersections

In this chapter we study problems about distributions of point counts for families of varieties cut out by pairs of polynomials taken from some vector space. That is, we study point count distributions for complete intersections of codimension 2. One approach to problems of this type makes use of the m-tuple weight enumerators analyzed in the previous chapter. We will consider del Pezzo surfaces of degree 4, which are isomorphic to the intersection of two quadrics in $\mathbb{P}^4$, using this framework and building on results of Chapter 2. One step in this process involves studying genus 1 curves arising as $(2,2)$-curves on $\mathbb{P}^1 \times \mathbb{P}^1$. This analysis is similar to the analysis of homogeneous quartics $w^2 = f_4(x,y)$ in $\mathbb{P}(2,1,1)$ carried out in Chapter 3. We end this chapter with some directions for future investigations.

1. Intersections of Two Conics in $\mathbb{P}^2(\mathbb{F}_q)$

In the first part of this thesis we saw how finding counts for the number of low-weight codewords of the dual of a code C can help to compute the weight enumerator of C. We begin this section by extending this idea to the 2-tuple weight enumerators of the previous chapter. This will tell us about common zeros of pairs of codewords drawn from C. Equivalently when C is a code coming from the evaluation of polynomials, this tells us about rational points on the intersections of the varieties cut out by these polynomials. The main idea will be to use the low-weight coefficients of $W_{C^\perp}^{[2]}(X,Y)$ to help compute $W_C^{[2]}(X,Y)$.

We prove the following result.

Theorem 113. *Let $C_{2,2} \subset \mathbb{F}_q^{q^2+q+1}$ be the 6-dimensional code coming from conics on $\mathbb{P}^2(\mathbb{F}_q)$. Then*

$$\begin{aligned}
W_{C_{2,2}}^{[2]}(X,Y) &= X^{q^2+q+1} + \frac{(q-1)q(q+1)^2(q^2+q+1)}{2} X^{2q+1}Y^{q^2-q} \\
&+ (q-1)^2q^3(q+1)(q^2+q+1)X^{q+2}Y^{q^2-1} \\
&+ (q-1)(q+1)(q^2+q+1)(2q^3-q^2-q+1)X^{q+1}Y^{q^2} \\
&+ \frac{(q-1)^4q^4(q+1)^2(q^2+q+1)}{24} X^4Y^{q^2+q-3} \\
&+ \frac{(q-1)^3q^4(q+1)^2(q^2+q+1)}{2} X^3Y^{q^2+q-2} \\
&+ \frac{(q-1)^2q^3(q+1)^2(q^2+q+1)(q^3-2q^2+7q-4)}{4} X^2Y^{q^2+q-1} \\
&+ \frac{(q^3-q)(q^3-1)(2q^6+q^5-2q^4+5q^3+6q^2-6q+3)}{6} XY^{q^2+q} \\
&+ \frac{(q-1)^3q^4(q+1)(q^2+q+1)(3q^2+1)}{8} Y^{q^2+q+1}.
\end{aligned}$$

We first proved this result by a very intricate analysis of all of the possible ways that two conics can intersect. For example, two conics can intersect in exactly two $\mathbb{F}_q$-rational points in several different ways. If both conics are smooth, they can be tangent at two distinct $\mathbb{F}_q$-rational points, or they can intersect at two $\mathbb{F}_q$-rational points and at two Galois-conjugate points defined over $\mathbb{F}_{q^2}$. We can count the number of pairs of conics that have each type of intersection. This becomes quite tedious, and here we avoid many of these intricacies.

PROOF. We break up $W_{C_{2,2}}^{[2]}(X,Y)$ by considering pairs of codewords that generate a $0, 1$ or 2 dimensional subspace of $\mathbb{F}_q^{q^2+q+1}$. That is,

$$W_{C_{2,2}}^{[2]}(X,Y) = W_{C_{2,2}}^{(0)}(X,Y) + (q^2-1)W_{C_{2,2}}^{(1)}(X,Y) + (q^2-1)(q^2-q)W_{C_{2,2}}^{(2)}(X,Y),$$

where $W_{C_{2,2}}^{(r)}(X,Y)$ is the rth support weight enumerator of $C_{2,2}$, defined in Section 4 of Chapter 5. We see that $W_{C_{2,2}}^{(0)}(X,Y) = X^{q^2+q+1}$ and that the 1st support

weight enumerator is $W^{(1)}_{C_{2,2}}(X,Y) = W_{C_{2,2}}(X,Y) - X^{q^2+q+1}$. Recall from Proposition 33 that

$$\begin{aligned} W_{C_{2,2}}(X,Y) &= X^{q^2+q+1} + \frac{(q^3-1)(q^2+q)}{2} X^{2q+1}Y^{q^2-q} \\ &\quad + (q^3-1)(q^3-q^2+1)X^{q+1}Y^{q^2} + \frac{(q^3-1)(q^2-q)}{2} XY^{q^2+q}. \end{aligned}$$

We need only determine the weight enumerator $W^{(2)}_{C_{2,2}}(X,Y)$. Given two distinct conics such that their corresponding codewords generate a 2-dimensional subspace of $\mathbb{F}_q^{q^2+q+1}$ there are relatively few possibilities for the size of their intersection. Either one conic is a double line and the other is a product of that line and another $\mathbb{F}_q$-rational line, or both conics are products of $\mathbb{F}_q$-rational lines and one of these lines is common to both conics, or the conics do not share a component and by Bézout's theorem the number of $\mathbb{F}_q$-points of the intersection is at most 4.

We count pairs of codewords c_1, c_2 that share a common line, L. First suppose that the variety corresponding to c_1 consists of the double line L. Then the variety corresponding to c_2 must consist of L together with another rational line, since these codewords span a two-dimensional space. The size of the intersection of these varieties is $q+1$. This happens in q^2+q ways.

Suppose the variety corresponding to c_1 consists of L together with a distinct line L_1. The variety corresponding to c_2 also consists of L together with a line L_2, possibly equal to L. If the intersection of L_1 and L_2 lies on L then the intersection has size $q+1$. This happens in $(q^2+q)q$ ways, since they must intersect at the common intersection point of L and L_1, but L_2 cannot be equal to L_1. Otherwise, the intersection of L_1 and L_2 is not on L, and these codewords have $q+2$ common zeros. This occurs in $(q^2+q)q^2$ ways. Therefore, we have determined all but 5 coefficients of $W^{(2)}_{C_{2,2}}(X,Y)$, but we also know the sum of these coefficients.

We have

$$\begin{aligned} W^{(2)}_{C_{2,2}}(X,Y) &= q^2(q^2+q+1)X^{q+2}Y^{q^2-1} + (q+1)(q^2+q+1)X^{q+1}Y^{q^2} \\ &+ c_4X^4Y^{q^2+q-3} + c_3X^3Y^{q^2+q-2} + c_2X^2Y^{q^2+q-1} \\ &+ c_1XY^{q^2+q} + c_0Y^{q^2+q+1}, \end{aligned}$$

where

$$c_0 + \cdots + c_4 = \frac{(q^6-1)(q^6-q)}{(q^2-1)(q^2-q)} - (q^2+q+1)^2 = (q^2+q+1)(q^5+q^3+q^2-1)q.$$

Now, as we did in the sketch of the proof of Theorem 3 in Chapter 2, we can create a 5×5 matrix where rows correspond to the terms of this expansion and columns correspond to powers of Y. We compute the first Y^k coefficient of $W^{[2]}_{C_{2,2}}(X,Y)$ for each $k \in [0,4]$ using the geometry of low-weight codewords of $C^{\perp}_{2,2}$. This gives a matrix M. Expanding all of the other terms of this weight enumerator under the MacWilliams transformation and subtracting gives a column vector that we call $\vec{b}$.

We note that the lowest weight codewords of $C^{\perp}_{2,2}$ have weight 4 and have support corresponding to 4 collinear points in $\mathbb{P}^2(\mathbb{F}_q)$. In fact, there are exactly

$$\frac{(q^2+q+1)(q+1)q(q-1)^2(q-2)}{24}$$

such codewords, $q-1$ times the number of collections of 4 collinear points in $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, the $X^{q^2+q-3}Y^4$ coefficient of $W^{[2]}_{C^{\perp}_{2,2}}(X,Y)$ is

$$(q^2-1)\frac{(q^2+q+1)(q+1)q(q-1)(q-2)}{24}.$$

Let $\vec{c}$ be a column vector with entries $c_0, \ldots, c_4$. Solving the resulting matrix equation gives $M \cdot \vec{c} = \vec{b}$, where

$$\vec{b} = \begin{pmatrix} (q+1)\cdot(q-1)^2\cdot q^2\cdot(q^2+q+1)\cdot(q^5+q^3+q^2-1) \\ (-1)\cdot(q+1)\cdot(q-1)^2\cdot q^2\cdot(q^2+q+1)\cdot(q^4+3q^3+q^2-q-1) \\ (-\frac{1}{2})\cdot(q-1)^2\cdot(q+1)^2\cdot q^3\cdot(q^2+q+1)\cdot(q^5+2q^4-4q^3-2q^2+q+1) \\ (-\frac{1}{6})\cdot(q+1)^2\cdot(q-1)^3\cdot q^3\cdot(q^2+q+1)\cdot(q^7+2q^6-7q^5-8q^4+7q^3+4q^2-q-1) \\ (-\frac{1}{24})\cdot(q+1)^2\cdot q^3\cdot(q-1)^4\cdot(q^2+q+1)\cdot(q^8-11q^7-10q^6+32q^5+24q^4-21q^3-9q^2+3q+2) \end{pmatrix}.$$

This completes the proof. □

The pairs of elements of $C_{2,2}^{\perp}$ such that the union of their support has size 4 give the Y^4 coefficient of $W_{C_{2,2}^{\perp}}^{[2]}(X,Y)$. Each pair of this type generates a 1-dimensional subspace of $C_{2,2}^{\perp}$. The lowest weight nonzero coefficient of $W_{C_{2,2}^{\perp}}^{(2)}(X,Y)$ comes from pairs of codewords such that the union of their supports of has size 5. Both of these codewords must have weight 4 or 5, which means their support must consist of collinear points. Two-dimensional subcodes of weight 6 must also have support consisting of collinear points. For weight 7 subcodes something new can happen. Consider the space spanned by two elements of weight 4 that share a common point in their support. The support now consists of 7 points lying on two lines. The fact that there are so few possibilities for the support of these low-weight subcodes makes it possible for us to analyze these cases in detail, but we will not do so here.

2. Del Pezzo Surfaces of Degree 4

In the previous section we studied the weight enumerator coming from the intersection of two quadrics in $\mathbb{P}^2(\mathbb{F}_q)$. The motivation for considering this particular example comes from the study of del Pezzo surfaces of degree 4.

The anti-canonical model of a del Pezzo surface of degree 4 is the intersection of two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$. Let $C_{4,2}$ be the 15-dimensional code of quadrics on $\mathbb{P}^4(\mathbb{F}_q)$. We can easily determine $W_{C_{4,2}}(X,Y)$. If we can compute $W_{C_{4,2}}^{[2]}(X,Y)$ then we will know the distribution of rational point counts for the intersection of two quadrics as

we vary through all q^{30} pairs. Given two quadrics f, g we can consider the pencil defined by this pair and the number of $\mathbb{F}_q$-points in its base locus. This is equivalent to knowing the number of points of the intersection.

The intersection of a generic pair of quadrics will be smooth, giving a del Pezzo surface of degree 4. In Chapter 2 we saw that a del Pezzo surface of degree 4 is given as the blow-up of $\mathbb{P}^2$ at 5 points. The resulting surface is smooth if and only if no three of these points lie on a line. The number of $\mathbb{F}_q$-points of this blow-up is given by Theorem 23, q^2+1 plus q times the trace of Frobenius acting on the Picard group of the surface. The Picard group is generated by the hyperplane class and the classes of five pairwise disjoint (-1)-curves on S. We note that there are 16 (-1)-curves on S. Frobenius fixes the hyperplane class and induces a permutation of these lines. This permutation is given by an element of the Weyl group of D_5, $W(D_5)$. By looking at the character table of D_5, as we did for E_6 and E_7 in Chapter 2, we determine the number of elements of $W(D_5)$ that have given trace.

Proposition 114. *Let $\pi \in W(D_5)$. Then $\mathrm{Tr}(\pi) \in [-3,5] \setminus \{4\}$. The number of elements of $W(D_5)$ with each trace value is given by the following table:*

Trace	-3	-2	-1	0	1	2	3	5
$\#W(D_5)$	25	80	420	864	430	80	20	1

.

Much like in Chapters 2 and 3 when we studied homogeneous quartics of the form $w^2 = f_4(x,y,z)$, there are a few kinds of intersections of quadrics that have singularities that are not simple. That is, the intersection can include a non-isolated singularity or an elliptic singularity. An example of the first case comes from intersecting any nonzero quadrics with a double hyperplane. For the second case we have a cone over a genus 1 curve. When studying cubic surfaces Elkies needed to study cones over genus 1 curves coming from cubic curves in $\mathbb{P}^2$ [**20**]. Earlier in this thesis we considered cones over genus 1 curves coming from double covers of $\mathbb{P}^1(\mathbb{F}_q)$

branched at four points, $w^2 = f_4(x, y)$. In this situation, the genus 1 curves arise come from $(2, 2)$-forms on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$.

In fact, every intersection of two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$ is either a del Pezzo surface of degree 4, possibly singular, a cone over a genus 1 curve, or has a non-isolated singularity. We can proceed in a similar manner to the case of double covers of $\mathbb{P}^2$ branched over a plane quartic. We can study the intersections with non-isolated singularities directly as we did at the end of Chapter 3 for del Pezzo surfaces of degree 2. We will study $(2, 2)$-curves on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ in the next section

We will then have 9 unknown coefficients to determine, one corresponding to each trace value in $[-3, 5]$, since a singular del Pezzo surface of degree 4 can have $q^2 + 5q + 1$ $\mathbb{F}_q$-points. We can attempt to find these coefficients by finding the first 9 coefficients of $W^{[2]}_{C_{4,2}}(X, Y)$ and applying the 2-tuple MacWilliams theorem that was used in the previous section.

There are other ways to study del Pezzo surfaces of degree 4 over finite fields. We begin by stating Theorem 8.6.2 in [**15**].

Theorem 115. *Let S be a del Pezzo surface of degree 4. The S is a complete intersection of two quadrics in $\mathbb{P}^4(\bar{\mathbb{F}}_q)$. Moreover, if S is nonsingular, then the equations of the quadrics can be reduced, after a linear change of variables to the diagonal forms*

$$\sum_{i=0}^{4} t_i^2 = \sum_{i=0}^{4} a_i t_i^2 = 0,$$

where $a_i \neq a_j$ for $i \neq j$.

The main idea here is that a smooth complete intersection of two quadrics can be simultaneously diagonalized. Unfortunately, this is not necessarily true over a non-algebraically closed field. However, we can still get a perfectly good, although somewhat restricted, code from this 5-dimensional space of diagonal quadrics intersected with a given smooth quadric.

Let C' denote the 5-dimensional code given by evaluation of the polynomials $\sum_{i=0}^{4} a_i t_i^2$ at the q^3+q^2+q+1 $\mathbb{F}_q$-points of the smooth quadric $t_0^2+\cdots+t_4^2$. Computing $W_{C'}(X,Y)$ would tell us quite a lot about the distribution of point counts for del Pezzo surfaces of degree 4 over $\mathbb{F}_q$.

We can actually consider a slightly more restricted version of this code. We evaluate these diagonal quadrics only at $\mathbb{F}_q$-points of the chosen smooth quadric $t_0^2+\cdots+t_4^2$. Therefore, adding multiples of this conic will not change the resulting codeword. This shows that we may assume $a_0 = 0$ and consider the resulting 4-dimensional code. This explains the restriction that the a_i are distinct in the statement of the theorem. If $a_i = a_j$ for some $i \neq j$ then adding $-a_i(t_0^2 + \cdots + t_4^2)$ will give a diagonal quadrics with at most 3 nonzero terms. All such quadrics are singular. It is not difficult to collect computational results on this 4-dimensional code for various values of q.

Alternatively, we could consider the 15-dimensional code of length $q^3 + q^2 + q + 1$ given by evaluating the entire space of quadrics in $\mathbb{P}^4(\mathbb{F}_q)$ at the set of $\mathbb{F}_q$-points of the chosen smooth diagonal quadric. This gives another way to approach this problem.

3. $(2,2)$-forms on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$

We recall that $\mathbb{P}^1(\mathbb{F}_q)\times\mathbb{P}^1(\mathbb{F}_q)$ is a smooth quadric in $\mathbb{P}^3(\mathbb{F}_q)$ with $(q+1)^2$ $\mathbb{F}_q$-points. There is another type of smooth quadric, a minus quadric, with only q^2+1 $\mathbb{F}_q$-points. A cone over a smooth conic in has $1+q(q+1) = q^2+q+1$ $\mathbb{F}_q$-points. There are also quadrics defined by the product of two planes. These planes can either be distinct $\mathbb{F}_q$-rational planes, Galois-conjugate planes, or a double plane such as $x^2 = 0$. We focus here on the smooth intersections of two quadrics in $\mathbb{P}^3(\mathbb{F}_q)$. In the case where one of these quadrics contains a plane we can determine the distribution of rational point counts by elementary means. We would eventually like to compute $W^{[2]}_{C_{3,2}}(X,Y)$, the 2-tuple weight enumerator for the code of quadrics on $\mathbb{P}^3(\mathbb{F}_q)$, but for now focus only on the code coming from the intersection of a conic with a chosen smooth quadric.

Consider the quadric given by $wz = xy$. This is a smooth quadric isomorphic to $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. A homogeneous quadratic polynomial in the variables (x, y, z, w) is determined by 10 coefficients. Let $[x_0 : x_1]$ and $[y_0 : y_1]$ give coordinates for the two factors of $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. We identify x with $x_0x_1,\ y$ with $y_0y_1,\ z$ with x_0y_1, and w with x_1y_1. This gives a q to 1 map from quadrics in $\mathbb{P}^3(\mathbb{F}_q)$ to equations of the form

$$(dy_0^2 + ey_0y_1 + fy_1^2)x_0^2 + (ay_0^2 + by_0y_1 + cy_1^2)x_0x_1 + (gy_0^2 + hy_0y_1 + iy_1^2)x_1^2 = 0,$$

where the 9 coefficients $a, b, c, \ldots, i \in \mathbb{F}_q$. For each of these q^9 equations we want to count $\mathbb{F}_q$-rational solutions of this equation in $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. Each such equation is homogeneous of degree 2 in the coordinates $[x_0 : x_1]$ and in the coordinates $[y_0 : y_1]$. An equation of this type is called a $(2, 2)$-form and the variety cut out by such a form is called a $(2, 2)$-curve. It is a standard result in algebraic geometry that a smooth (a, b)-curve on $\mathbb{P}^1 \times \mathbb{P}^1$ has genus $(a - 1)(b - 1)$. When this $(2, 2)$-form cuts out a smooth subvariety of $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ it is a genus 1 curve and we can use methods from Chapter 3 to understand the distribution of point counts.

In order to determine the number of zeros of a $(2, 2)$-form written this way we think of it as a quadric in x_0, x_1 and use the quadratic formula. Consider $ax_0^2 + bx_0x_1 + cx_1^2$. The number of zeros is $0, 1$ or 2 depending on whether the discriminant $b^2 - 4ac$ is a non-square, zero, or a nonzero square, respectively. We evaluate the form at each of the $q + 1$ points $[y_0 : y_1]$, and for each we count solutions for the resulting quadratic equation. The case where we have to do more than just count the number of times $b^2 - 4ac$ is a square is when a, b, c are all simultaneously equal to zero. In this case $b^2 - 4ac = 0$, but we actually have $q + 1$ solutions for our form, one for each point $[x_0 : x_1]$.

The coefficients are quadratic polynomials in y_0 and y_1 so that $b^2 - 4ac$ is equal to the homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$

$$\begin{aligned} & (a^2 - 4dg)y_0^4 + (2ab - 4eg - 4dh)y_0^3 y_1 + (b^2 + 2ac - 4fg - 4eh - 4di)y_0^2 y_1^2 \\ + \quad & (2bc - 4fh - 4ei)y_0 y_1^3 + (c^2 - 4fi)y_1^4. \end{aligned}$$

Therefore, we are really interested in the distribution of rational points on equations of the form $w^2 = f_4(y_0, y_1)$ where $f_4(y_0, y_1)$ is a homogeneous quartic on $\mathbb{P}^1(\mathbb{F}_q)$. We studied this problem in depth in Chapter 3. In this section we only consider the quartics with distinct roots, the case where the resulting variety in $\mathbb{P}(2, 1, 1)$ is an elliptic curve.

The following result is the analogue of Proposition 44 in Chapter 3.

Proposition 116. *Let E be an elliptic curve defined over $\mathbb{F}_q$ with $q+1-t$ $\mathbb{F}_q$-rational points. The number of $(2,2)$-forms on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ that give a zero set isomorphic to E is*

$$\frac{(q-1)(q-t)|\mathrm{PGL}_2(\mathbb{F}_q)|^2}{|\mathrm{Aut}(E)|} = \frac{(q-t)(q-1)^3 q^2 (q+1)^2}{|\mathrm{Aut}(E)|}.$$

Proof. Let E be an elliptic curve over $\mathbb{F}_q$ embedded in $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ as a $(2,2)$-curve. The embedding comes with a projection to each $\mathbb{P}^1(\mathbb{F}_q)$. Taking the inverse image of a point on one of these factors gives a degree 2 divisor class. The divisor class comes from looking at the lines of each ruling. We claim that these two divisor classes from the projections, D_1 and D_2, cannot be linearly equivalent.

Suppose that $D_1 \sim D_2$ and let p be an $\overline{\mathbb{F}}_q$-rational point of E such that $2p \not\sim D_1$. Let π_1 be the projection to the first $\mathbb{P}^1(\mathbb{F}_q)$ and π_2 the projection to the second. Then there are points q and r on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ such that $\pi_1^{-1}(x) = p+q$ and $\pi_2^{-1}(y) = p+r$. The points p and q lie on the same line from one ruling of $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ and p and r lie on the same line of the other ruling. Since $D_1 \sim D_2$ each fiber of the projections is in the same divisor class. Therefore $p + q \sim p + r$, which implies $q \sim r$. We conclude

that $q = r$. Since a pair of lines from different rulings of $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ intersect at only one point, we have $p = q = r$. This contradicts the assumption that $2p \not\sim D_1$, and therefore $D_1 \not\sim D_2$.

We count the number of degree 2 divisor classes on E. We recall that for each d, $|\mathrm{Pic}_d(E)| = |E(\mathbb{F}_q)|$. Therefore, the number of degree 2 divisors of E is equal to the number of $\mathbb{F}_q$-points of E, $q + 1 - t$. By the Riemann-Roch theorem, a divisor class of degree 2 has a two-dimensional space of sections. Choosing a basis gives a map to $\mathbb{P}^1(\mathbb{F}_q)$. This map is defined only up to automorphisms of $\mathbb{P}^1(\mathbb{F}_q)$.

Starting with a $(2,2)$-curve E embedded in $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ with two distinct degree 2 divisor classes D_1, D_2, we take the map that forgets the divisor classes. This takes (E, D_1, D_2) to E, a $(2,2)$-curve. The size of a fiber of this map is $\frac{(q+1-t)(q-t)}{|\mathrm{Aut}(E)|}$, where the first two terms come from choices of divisor classes and the last from automorphisms of E that fix the identity element of E. □

Recall the assumption that the characteristic of $\mathbb{F}_q$ is not 2 or 3.

Corollary 117. *Let $j \in \mathbb{F}_q$. The number of $(2,2)$-forms in $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ with j-invariant equal to j is $(q-1)^3 q^3 (q+1)^2$.*

The number of equations of the form $y^2 = f(x)$ with $f(x)$ a quartic polynomial of j-invariant equal to j is $(q-1)^2 q(q+1)$.

Proof. The number of isomorphism classes of elliptic curves with given j-invariant is equal to the size of the automorphism group of any such curve. We consider a curve E with $q + 1 - t$ $\mathbb{F}_q$-points together with its quadratic twist, a curve of the same j-invariant with $q + 1 + t$ points. We sum

$$\frac{(q-1)^3 q^2 (q+1)^2 (q - t + q + t)}{|\mathrm{Aut}(E)|},$$

over all such pairs of isomorphism classes with given j-invariant. We add curves with exactly $q + 1$ $\mathbb{F}_q$-points separately. This proves the first statement.

For the second statement, we sum $\frac{(q-1)^2 q(q+1)}{|\mathrm{Aut}(E)|}$ over these isomorphism classes. $\square$

Proposition 118. *Suppose that $y^2 = f(x)$ gives the equation of an elliptic curve over $\mathbb{F}_q$ with $q+1-t$ rational points. Then the number of ways that this quartic arises as the discriminant of a $(2,2)$-form is $(q-t)(q-1)q(q+1)$.*

Proof. We recall from the proof of Proposition 44 that writing E as $w^2 = f_4(x,y)$ is equivalent to choosing a single degree 2 divisor class on E. In order to write E as the zero set of a $(2,2)$-form we must choose another distinct divisor class and a basis of sections for it, which we can do in $(q-t)|\mathrm{PGL}_2(\mathbb{F}_q)|$ ways. $\square$

We must pay special attention to curves with j-invariant 0 and 1728 just as we did in Chapter 3. The facts we need are exactly the content of Proposition 42. The values of $N(t)$ are given in Lemma 48. Again, we emphasize that the characteristic of $\mathbb{F}_q$ is not equal to 2 or 3.

We determine the weight enumerator from $(2,2)$-forms on $\mathbb{P}^1(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ that have zero set isomorphic to a smooth genus 1 curve. This is the analogue of Proposition 45 for $(2,2)$-forms.

Proposition 119 (Smooth part)**.** *Fix $q = p^f$ with $p \neq 2, 3$ and recall the function $N(t)$, the number of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with exactly $q+1-t$ points.*

Let

$$W'_{2,2}(X,Y) = \sum_{t=\lceil -2\sqrt{q} \rceil}^{\lfloor 2\sqrt{q} \rfloor} N(t)(q-1)^3 q^2 (q+1)^2 \frac{q-t}{2} X^{q+1-t} Y^{(q+1)^2-(q+1-t)}.$$

If $\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right) = -1$, then the contribution to the weight enumerator from $(2,2)$-forms that have zero set isomorphic to a smooth genus 1 curve is $W'_{2,2}(X,Y)$.

If $p \equiv 1 \pmod 3$, *let* (a,b) *be any pair of integers with* $p \nmid a$ *and* $a^2 - ab + b^2 = q$. *Then let*

$$P_0(X,Y) = \sum_{t' \in T_0} \frac{(q-1)^3 q^2 (q+1)^2 (q-t')}{3} X^{q+1-t'} Y^{(q+1)^2-(q+1-t')}$$

where $T_0 = \{\pm(2a-b), \pm(a+b), \pm(2b-a)\}$.

If $p \equiv 2 \pmod 3$ *and* f *is even, then let*

$$\begin{aligned} P_0(X,Y) &= \frac{(q-1)^3 q^2 (q+1)^2}{3} \Big((q - 2\sqrt{q}) X^{q+1-2\sqrt{q}} Y^{(q+1)^2-(q+1-2\sqrt{q})} \\ &+ (q + 2\sqrt{q}) X^{q+1+2\sqrt{q}} Y^{(q+1)^2-(q+1+2\sqrt{q})} \\ &+ 2(q - \sqrt{q}) X^{q+1-\sqrt{q}} Y^{(q+1)^2-(q+1-\sqrt{q})} \\ &+ 2(q + \sqrt{q}) X^{q+1+\sqrt{q}} Y^{(q+1)^2-(q+1+\sqrt{q})} \Big). \end{aligned}$$

Otherwise, let $P_0(X,Y) = 0$.

If $p \equiv 1 \pmod 4$, *let* (a,b) *be any pair of integers with* $p \nmid a$ *and* $a^2 + b^2 = q$. *Then let*

$$\begin{aligned} P_{1728}(X,Y) &= \frac{(q-1)^3 q^2 (q+1)^2}{4} \Big((q - 2a) X^{q+1-(2a)} Y^{(q+1)^2-(q+1-2a)} \\ &+ (q + 2a) X^{q+1+(2a)} Y^{(q+1)^2-(q+1+2a)} + (q - 2b) X^{q+1-(2b)} Y^{(q+1)^2-(q+1-2b)} \\ &+ (q + 2b) X^{q+1+(2b)} Y^{(q+1)^2-(q+1+2b)} \Big). \end{aligned}$$

If $p \equiv 3 \pmod 4$ *and* f *is even, let*

$$\begin{aligned} P_{1728}(X,Y) &= \frac{(q-1)^3 q^2 (q+1)^2}{4} \Big((q - 2\sqrt{q}) X^{q+1-2\sqrt{q}} Y^{(q+1)^2-(q+1-2\sqrt{q})} \\ &+ (q + 2\sqrt{q}) X^{q+1+2\sqrt{q}} Y^{(q+1)^2-(q+1+2\sqrt{q})} + 2q X^{q+1} Y^{(q+1)^2-(q+1)} \Big). \end{aligned}$$

Otherwise let $P_{1728}(X) = 0$.

The contribution to the weight enumerator from $(2,2)$*-forms that have zero set isomorphic to a smooth genus* 1 *curve is*

$$W'_{2,2}(X,Y) - P_0(X,Y) - P_{1728}(X,Y).$$

This weight enumerator is a useful piece in determining any of the weight enumerators coming from intersections of quadrics in $\mathbb{P}^4(\mathbb{F}_q)$ defined in the previous section.

4. Further Directions

In future work we intend to carry out the strategy described in this chapter to compute the weight enumerators coming from intersections of two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$. We also note that other families of del Pezzo surfaces can be studied using these ideas. For example, a smooth del Pezzo surface of degree 5 is isomorphic to a linear section of the Grassmannian of lines in $\mathbb{P}^4$, and this Grassmannian can be defined in terms of the five Pfaffians of the 4×4 minors of a skew-symmetric 5×5 matrix [**15**]. It seems that issues related to the intersections of varieties cut out by these Pfaffians could arise.

Del Pezzo surfaces of degree 1 can also be studied as varieties in a certain weighted projective space. Consider the weighted projective space $\mathbb{P}(1,1,2,3)$ with coordinates $[w:x:y:z]$ where x and y have degree 1, z has degree 2, and w has degree 3. A del Pezzo surface of degree 1 is given by a homogeneous sextic equation of the form

$$w^2 + z^3 + L(x,y)wz + H(x,y)w = Q(x,y)z^2 + G(x,y)z + F(x,y),$$

where $H(x,y), L(x,y), Q(x,y), G(x,y)$ and $F(x,y)$ are homogeneous polynomials of degrees $1, 3, 2, 4$, and 6, respectively. Varying the coefficients of such forms gives q^{16} total equations, and adding coefficients to the w^2 and z^3 terms gives an 18-dimensional linear code. The relevant Weyl group here is $W(E_8)$, and the conditions for 8 points in $\mathbb{P}^2$ to be in general position are more complicated than what we have

seen previously. These varieties are more complicated than the homogeneous quartics in $\mathbb{P}(2,1,1,1)$ that occur for del Pezzo surfaces of degree 2, so studying the weight enumerator of these sextics is likely to be quite challenging. If the characteristic of $\mathbb{F}_q$ is not equal to 2 or 3 we may suppose that $H(x,y) = Q(x,y) = 0$, making things slightly easier.

There is no real conceptual reason why we need to avoid characteristic 2 and 3 in the type of analysis given in this thesis. In future work we would like to remove this restriction for the study of del Pezzo surfaces of degree 2. For characteristic 2 we need to consider homogeneous quartics in $\mathbb{P}(2,1,1,1)$ of the form

$$\alpha w^2 + f_2(x,y,z)w + f_4(x,y,z) = 0,$$

where $f_2(x,y)$ is a homogeneous quadratic polynomial on $\mathbb{P}^1(\mathbb{F}_q)$. This is a 22-dimensional code. This may make finding the counts for low-weight dual codewords more complicated, but similar techniques should work.

We also need to adapt results for cones over genus 1 curves in the case where the characteristic is 2 or 3. In Chapter 3, when studying varieties of the form $w^2 = f_4(x,y)$ we used the fact that an elliptic curve with j-invariant not equal to 0 or 1728 has exactly 2 automorphisms, and that these two special j-invariants can have curves with 6 and 4 automorphisms, respectively. Over fields of characteristic 2 and 3 there can be curves with 24 and 12 automorphisms, respectively. We will have to analyze these curves with extra automorphisms more carefully.

We would like to extend this analysis to deal with codes coming from curves of higher genus. For example, it is easy to compute the weight enumerator of homogeneous sextics on $\mathbb{P}^1(\mathbb{F}_q)$. The double cover of $\mathbb{P}^1(\mathbb{F}_q)$ branched at six points gives a variety in the weighted projective space $\mathbb{P}(2,1,1)$, $w^2 = f_6(x,y)$ that is generically a genus 2 curve. If we could compute $\mathrm{QR}_{C_{1,6}}(X, X^2, 1)$ for this 7-dimensional code, then we would understand point count distributions for genus 2 curves over $\mathbb{F}_q$. There

will be some new difficulties here. For example, Deuring's result gives the number of isomorphism classes of genus 1 curves with $q + 1 - t$ rational points over $\mathbb{F}_q$ in terms of a Dedekind class number. Since the set of rational points of a curve of genus $g > 1$ does not form a group one will most likely have to study the Jacobian of the curve, an abelian variety of dimension g. In the genus 2 case there are more kinds possibilities the endomorphism ring of the Jacobian of C and we would need to carefully analyze how often these different structures arise. For genus greater than 2 many new difficulties from the theory of abelian varieties will arise.

We would also like to investigate whether other weight enumerators and variations of the MacWilliams theorem can be useful in studying point count distributions for varieties over finite fields. There are many other weight enumerators to consider, for example complete weight enumerators and more complicated weight enumerators from m-tuples of codewords, but the MacWilliams identities for these become much more complicated. In future work we intend to investigate how far this approach can be taken.

Bibliography

[1] A. Barg, The matroid of supports of a linear code. Appl. Algebra Engrg. Comm. Comput. 8 (1997), no. 2, 165-172.

[2] F. Bars, On the automorphisms groups of genus 3 curves. Notes del Seminari de Teoria Nombres, UB-UAB-UPC 2004/05: Genus 3 curves. Barcelona, Gener 2005, http://mat.uab.es/ francesc/mates/autgen3.pdf.

[3] B. Birch, How the number of points of an elliptic curve over a fixed prime field varies. J. London Math. Soc. 43 (1968), 57-60.

[4] M. I. Boguslavsky, Sections of del Pezzo surfaces, and generalized weights. Problems of Information Transmission, 34 (1998), no. 1, 14-24.

[5] M. I. Boguslavsky, Lattices, codes, and Radon transforms. Thesis (Ph.D.)-University of Amsterdam. 1999. 67 pp.

[6] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), 235265.

[7] T. Britz, MacWilliams identities and matroid polynomials. Electron. J. Combin. 9 (2002), no. 1, Research Paper 19, 16 pp. (electronic).

[8] T. Britz, Code enumerators and Tutte polynomials. IEEE Trans. Inform. Theory 56 (2010), no. 9, 4350-4358.

[9] J. W. Bruce and P. J. Giblin, A stratification of the space of plane quartic curves. Proc. London Math. Soc. (3) 42 (1981), no. 2, 270-298.

[10] L. Clozel, M. Harris, and R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. Publ. Math. Inst. Hautes Études Sci. No. 108 (2008), 1-181.

[11] I. Connell, Elliptic curve handbook. 1996, http://pendientedemigracion.ucm.es/BUCM/mat/doc8354.pdf.

[12] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups. Springer-Verlag, New York 1999.

[13] A. Couvreur, The dual minimum distance of arbitrary-dimensional algebraic-geometric codes. J. Algebra 350 (2012), 84-107.

[14] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkrper. Abh. Math. Sem. Hansischen Univ. 14 (1941). 197-272.

[15] I. Dolgachev, Classical algebraic geometry: A modern view. Cambridge University Press, Cambridge, 2012.

[16] I. Dolgachev. Weighted projective varieties. In Group actions and vector fields (Vancouver, B.C., 1981), 34-71, Lecture Notes in Math., 956, Springer, Berlin, 1982.

[17] S. Dougherty and S. Han, Higher weights and generalized MDS codes. J. Korean Math. Soc. 47 (2010), no. 6, 1167-1182.

[18] M. Eastwood, Moduli of isolated hypersurface singularities. Asian J. Math. 8 (2004), no. 2, 305-313.

[19] D. Eisenbud, M. Green, and J. Harris, Cayley-Bacharach theorems and conjectures. Bull. Amer. Math. Soc. (N.S.) 33 (1996), no. 3, 295-324.

[20] N. D. Elkies, Linear codes and algebraic geometry in higher dimensions. Preprint, 2006.

[21] N. D. Elkies. The Klein quartic in number theory. In The eightfold way, 51-101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[22] C. Fontanari and C. Marcolla, On the geometry of small weight codewords of dual algebraic geometric codes, 2011, http://arxiv.org/abs/1104.1320.

[23] D. G. Glynn, Ring of geometries II. J. Combin. Theory Ser. A 49 (1988), no. 1, 26-66.

[24] R. Hartshorne, Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[25] D. R. Heath-Brown, Kummer's conjecture for cubic Gauss sums. Israel J. Math. 120 (2000), part A, 97-124.

[26] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[27] K. Ireland and M. Rosen, A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[28] T. Kløve, Support weight distribution of linear codes. Discrete Math. 106/107 (1992), 311-316.

[29] S. Lang, Sur les séries L d'une variété algébrique. Bull. Soc. Math. France 84 (1956), 385-407.

[30] S. Lang, Elliptic functions. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[31] S. Li, Rational points on del Pezzo surfaces of degree 1 and 2. Thesis (Ph.D.)-Rice University. 2010. 78 pp.

[32] D. Loughran, Manin's conjecture for del Pezzo surfaces, Thesis (Ph.D.)-University of Bristol. 2011. 126 pp.

[33] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code. Bell System Tech. J. 42 (1963), 79-94.

[34] F. J. MacWilliams and N. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Company, New York, 1977.

[35] Y. Manin, Cubic forms: Algebra, geometry, arithmetic. Translated from the Russian by M. Hazewinkel. Second edition. North-Holland Mathematical Library, 4. North-Holland Publishing Co., Amsterdam, 1986.

[36] S. Meagher and J. Top, Twists of genus three curves over finite fields. Finite Fields Appl. 16 (2010), no. 5, 347-368.

[37] S. Miller. and R. Murty, Effective equidistribution and the Sato-Tate law for families of elliptic curves. J. Number Theory 131 (2011), no. 1, 25-44.

[38] G. Nebe, E. Rains, and N. Sloane, *Self dual codes and invariant theory*, Algorithms and Computation in Mathematics, 17. Springer-Verlag, Berlin, 2006.

[39] D. Ray-Chaudhuri and I. Siap, On r-fold complete weight enumerators of r linear codes. Algebra and its applications (Athens, OH, 1999), 501-513, Contemp. Math., 259, Amer. Math. Soc., Providence, RI, 2000.

[40] R. Schoof, Nonsingular plane cubic curves over finite fields. J. Combin. Theory Ser. A 46 (1987), no. 2, 183-211.

[41] K. Shiromoto, A new MacWilliams type identity for linear codes. Hokkaido Math. J. 25 (1996), no. 3, 651-656.

[42] I. Siap, Generalized r-fold weight enumerators for linear codes and new linear codes with improved minimal distances. Thesis (Ph.D.)-The Ohio State University. 1999. 158 pp.

[43] J. Silverman. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[44] J. Simonis, The effective length of subcodes, Appl. Algebra Engrg. Comm. Comput. 5 (1994), no. 6, 371-377.

[45] W. Stein et al. Sage Mathematics Software (Version 4.8), The Sage Development Team, 2012, http://www.sagemath.org.

[46] L. Z. Tang, Algebraic geometry codes of curves of complete intersection. Sci. China Ser. A 37 (1994), no. 8, 909-923.

[47] L. Z. Tang, On the weight hierarchy of codes associated to curves of complete intersection. J. Pure Appl. Algebra 105 (1995), no. 3, 307-317.

[48] A. Terras, *Fourier analysis on finite groups and applications*, Cambridge University Press, New York, 1999.

[49] M. A. Tsfasman and S. G. Vlăduţ, Geometric approach to higher weights. IEEE Trans. Inform. Theory 41 (1995), no. 6, part 1, 1564-1588.

[50] Z. Wan, The weight hierarchies of the projective codes from nondegenerate quadrics. Des. Codes Cryptogr. 4 (1994), no. 3, 283-300.

[51] Z. Wan and X. Wu, The weight hierarchies and generalized weight spectra of the projective codes from degenerate quadrics. Discrete Math. 177 (1997), no. 1-3, 223-243.

[52] W. C. Waterhouse, Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4) 2 (1969), 521-560.

[53] V. K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Infom. Theory 37 (1991), no. 5, 1412-1418.